Part No. 210676-C
March 2001

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Business Policy Switch 2000 Software Version 1.1

* 2 1 0 6 7 6 - C *

NORTEL
NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. March 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

BaySecure, BayStack, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, Optivity, and Passport are trademarks of Nortel Networks.

Microsoft and Windows are trademarks of Microsoft Corporation.

Java is a trademark of Sun Micorsystems, Inc.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Contents

Introduction 5

Related publications 5

New features and enhancements 7

- Compatibility with BayStack 450 Switch software version 4.0 7
- QoS traffic policing 7
  - Introduction 8
  - QoS and configuring filters 9
  - Configuring using the Web-based management system 9
- EAPOL-based security 15
  - Introduction 15
  - EAPOL-based security example 16
  - Overview and terms 17
  - EAPOL dynamic VLAN assignment 19
  - Setting up the Authentication server 20
  - Authentication process 20
  - System requirements 22
  - EAPOL-based security configuration rules 23
  - RADIUS-based network security 23
  - Configuring EAPOL using CI menus 24
  - Configuring EAPOL using JDM 28
  - Configuring EAPOL using the Web-based management system 39
- Support for the GBIC MDA 43
- Automatic PVID 43
  - Introduction 44
  - PVID/VLAN association example 44
  - Configuring Automatic PVID using CI menus 45
  - Configuring Automatic PVID using the Web-based management system 49
- Tabular port statistics 53
- Ability to ping 54

Improved STP Fast Learning Mode 54
BootP menu item for a stack of only BPS 2000 switches 54
Additional Web-based management operation 55
Access to the Web-based management system using JDM 55
Additional Java security 57
MAC address-based security 57
Resolved issues 65
Known issues 65
Version 1.1 issues 65
Known limitations 66

Introduction

These release notes for the Nortel Networks Business Policy Switch 2000* software version 1.1 provide information about software and operational issues not included in the Business Policy Switch 2000 (BPS 2000) software version 1.0 and version 1.0.1 guides.

To obtain the software version 1.1, download the following files from the Customer Support World Wide Web site:

- bps2k110.img (software file)
- bps2k110.bin (diagnostics file)

To obtain the Java* Device Manager (DM) software to manage the BPS 2000, download the following file from the Customer Support World Wide Web site:

- JDM 5.1.0.0

These release notes provide information on version 1.1 and cover the following topics:

- "Related publications," next
- "New features and enhancements" on page 7
- "Resolved issues" on page 65
- "Known issues" on page 65
- "Known limitations" on page 66

Related publications

For more information about the BPS 2000 switch, refer to:

- *Release Notes for the Business Policy Switch 2000 Software version 1.0.1* (part number 210676-B)
- *Addendum to the Release Notes for the Business Policy Switch 2000* (part number 210676-A)
- *Release Notes for the Business Policy Switch 2000* (part number 209320-A)

- *Using the Business Policy Switch 2000* (part number 208700-A)
- *Using Web-Based Management for the Business Policy Switch 2000* (part number 209570-A)
- *Reference for the Business Policy Switch 2000 Management Software* (part number 209322-A)
- *Getting Started with the Business Policy Switch 2000 Management Software* (part number 209321-A)
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A)
- *Installing Media Dependent Adapters (MDAs)* (part number 302403-F)
- *Managing Policy Information in Optivity Policy Services for Business Policy Switch* (part number 306969-D)
- *Installing Optivity Policy Services for Business Policy Switch* (part number 306972-C)
- *Task Map - Installing the OPS for BPS Product Family* (part number 306976-C)
- *Release Notes for Optivity Policy Services for the Business Policy Switch Version 1.0* (part number 306975-C)
- *Known Anomalies for Optivity Policy Services for the Business Policy Switch Version 1.0* (part number 306974-C)
- *Using the Optivity Quick2Config 2.2 Client Software* (part number 207810-B)
- *Installing and Administering Optivity Quick2Config 2.2* (part number 207809-B)
- *Configuring Business Policy Switches with Optivity Quick2Config 2.2* (part number 311208-A)
- *Release Notes for Optivity Quick2Config for Business Policy Switch 2000, v.2.2.1* (part number 310621-A)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www25.nortelnetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

New features and enhancements

The following paragraphs describe the new features and enhancements offered with the BPS 2000 software version 1.1:

- "Compatibility with BayStack 450 Switch software version 4.0," next
- "QoS traffic policing" on page 7
- "EAPOL-based security" on page 15
- "Support for the GBIC MDA" on page 43
- "Automatic PVID" on page 43
- "Ability to ping" on page 54
- "Tabular port statistics" on page 53
- "Improved STP Fast Learning Mode" on page 54
- "BootP menu item for a stack of only BPS 2000 switches" on page 54
- "Additional Web-based management operation" on page 55

Compatibility with BayStack 450 Switch software version 4.0

The software version 1.1 for the BPS 2000 is compatible with version 4.0 for the BayStack 450 Switch.

When you are using these two switches combined in a stack configuration, ensure that both are running the latest software version (BPS 2000 version 1.1 and BayStack 450 version 4.0.). The Main Menu of the Console Interface (CI) menus shows an Interoperability Software Version Number (ISVN). For the latest releases, the ISVN is 2 for both the BayStack 450 and BPS 2000 switches.

QoS traffic policing

For more information on Quality of Service (QoS) and the BPS 2000 as well as sample QoS configurations, refer to *Using Web-Based Management for the Business Policy Switch 2000* and *Release Notes for the Business Policy Switch 2000.*

This section contains the following information on QoS traffic policing:

- "Introduction," next
- "QoS and configuring filters" on page 9
- "Configuring using the Web-based management system" on page 9

Introduction

The BPS 2000 switch can interoperate with the Nortel Networks Optivity* Policy Server using Common Open Policy Services (COPS). For information about Optivity, go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product (in this case, Optivity Network Management and IP Services section).

QoS traffic policing, which operates at ingress, provides different levels of service to data streams through user configurable parameters. An example would be to limit traffic entering a port to a specified bandwidth, such as 25 Kb/s (Committed Rate). Instead of dropping all traffic that exceeds this threshold, traffic policing allows you to configure a Committed Burst Rate to exceed the threshold (Committed Rate), for a brief period of time, without being dropped.

The BPS 2000 filters collectively can take the following actions on a packet, depending on your configuration:

- Pass or Drop
- Re-mark the packet when Pass is selected
    - Re-mark a new DiffServ Codepoint (DSCP)
    - Re-mark the 802.1p field
    - Mark the Drop precedence

You must use either SNMP or the Web-based management system to configure the traffic policing filters. You can also configure traffic classifiers without traffic policing, in which case you choose No Metered Data in the Data Specification field of the Meter page.

Because the number of filters available in hardware is limited, Nortel Networks provides some design guidelines for constructing traffic policing.

QoS and configuring filters

You can install filters that will act on traffic destined for the switch itself, such as ICMP Echo Requests (ping) and SNMP messages. If the associated action is to drop the traffic, you can lock yourself out of the switch.

However, traffic destined for the switch and received through a port on the base unit of a stack is not dropped even if filters targeting the traffic are installed and drop has been specified. This behavior prevents you from completely isolating yourself from the switch. Consider this behavior when you configure filters and when you allocate ports for the purposes of configuring and or monitoring the switch.

Also, please note when configuring IP filters, the Address Mask specifies the portion of the address used to determine if that particular packet meets your filter criteria.

Configuring using the Web-based management system

You can configure traffic policing using SNMP or the Web-based management system. Refer to *Using Web-Based Management for the Business Policy Switch 2000* for more information on using the following QoS Advanced pages: IP Classification, Layer2 Classification, Actions, and Interface Group.

You will need to configure traffic policing using the following pages in the following order:

1 From the main menu, choose one of the following:

   - Application > QoS > QoS Advanced > Rules > IP Classification

---

Note: After configuring an IP filter, the screen may return the message:
`Submit Failed!`
Double-check that you have correctly entered the Destination Address Mask and the Source Address Mask. The Address Mask specifies that portion of the address used to determine if the packet meets the filter criteria; the Address Mask is *not* a subnet mask.
If you specify a subnet address, ensure that the host portion of the address contains a 0 value.
If you intend to identify an IP host address, ensure that the Address Mask is 255.255.255.255.

- Application > QoS > Advanced QoS > Rules > Layer2 Classification

2 Configure the filter and the filter group.

  a The filter

  b The filter group

3 Click Submit.

4 Choose Application > QoS > QoS Advanced > Actions page.

  a Create and name an In-Profile Action.

  b If you plan to work with metered data, create and name your own Out-Profile Action.

Note: When configuring an In-Profile action you must take at least one of the following actions:
- Change the DSCP value in the Update the DSCP field
- Choose from the Set Drop Precedence list
- Choose from the Update Priorities list

---

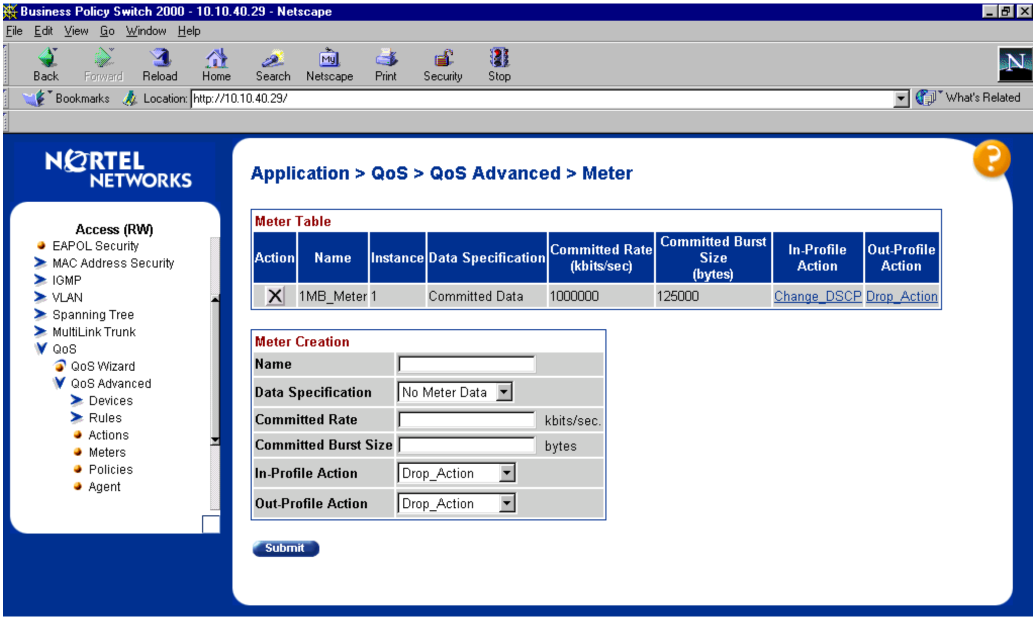
5 Click Submit

6 Choose Application > QoS > QoS Advanced > Meter.

> **Note:** You cannot edit Meters. To change the Meter, you must first delete the current Meter and create the one you want.

The Meter page opens (Figure 1).

Figure 1 Meter page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
EAPOL Security
MAC Address Security
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
QoS Wizard
QoS Advanced
Devices
Rules
Actions
Meters
Policies
Agent
Submit

Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (kbits/sec)	Committed Burst Size (bytes)	In-Profile Action	Out-Profile Action
☒	1MB_Meter	1	Committed Data	1000000	125000	Change_DSCP	Drop_Action

Meter Creation

Name		
Data Specification	No Meter Data	
Committed Rate		kbits/sec.
Committed Burst Size		bytes
In-Profile Action	Drop_Action	
Out-Profile Action	Drop_Action	

7 In the Meter Creation area, create the traffic policing meters.

Table 1 describes the fields in the Meter Creation area, which you use to set new meters.

Table 1 Meter Creation fields

Field	**Description**
Name	Enter the name for the filter you are creating.
Data Specification	Choose from the list to install a filter with: • No Meter Data • Metered Data NOTE: When you choose No Meter Data, do not complete the Committed Rate, Committed Burst Size, or Out-Profile Action fields in the box.
Committed Rate	Use this field **only** if you specified metered data for this filter (refer to Data Specification, above). Enter the Committed Rate in kbits/second here. You can enter from 13 kbits/second to 1,700,000 kbits/second.
Committed Burst Size	Use this field **only** if you specified metered data for this filter (refer to Data Specification, above). Enter the Committed Burst Size in bytes here. You can enter from 2,047 bytes to 131,071 bytes.
In-Profile Action	Choose from the list the action you previously created (using the Actions page).
Out-Profile Action	Use this field **only** if you specified metered data for this filter (refer to Data Specification, above). Choose from the list the action you previously created (using the Actions page).

8 View created meters in the Meter Table.

Table 2 describes the fields in the Meter Table.

Table 2 Meter Table fields

Field	**Description**
Action	Deletes that meter.
Name	Displays the name of the filter.
Instance	Displays the generated Meter Table index.
Data Specification	Displays whether the filter is set up with Metered Data or No Meter Data.
Committed Rate	Displays the specified bandwidth, in kbits per second.

Table 2 Meter Table fields (continued)

Field	Description
Committed Burst	Displays the specified bytes allowed to exceed the threshold set in the Committed Rate field for a brief period.
In-Profile Action	Displays the action (configured on the Actions page) for the switch to take on In-Profile traffic, which is traffic within the Committed Rate.
Out-Profile Action	Displays the action (configured on the Actions page) for the switch to take on Out-of-Profile traffic, which is that exceeds the Committed Rate as well as the Committed Burst Size. This field is unused for filters with No Meter Data defined.

9 Click Submit.

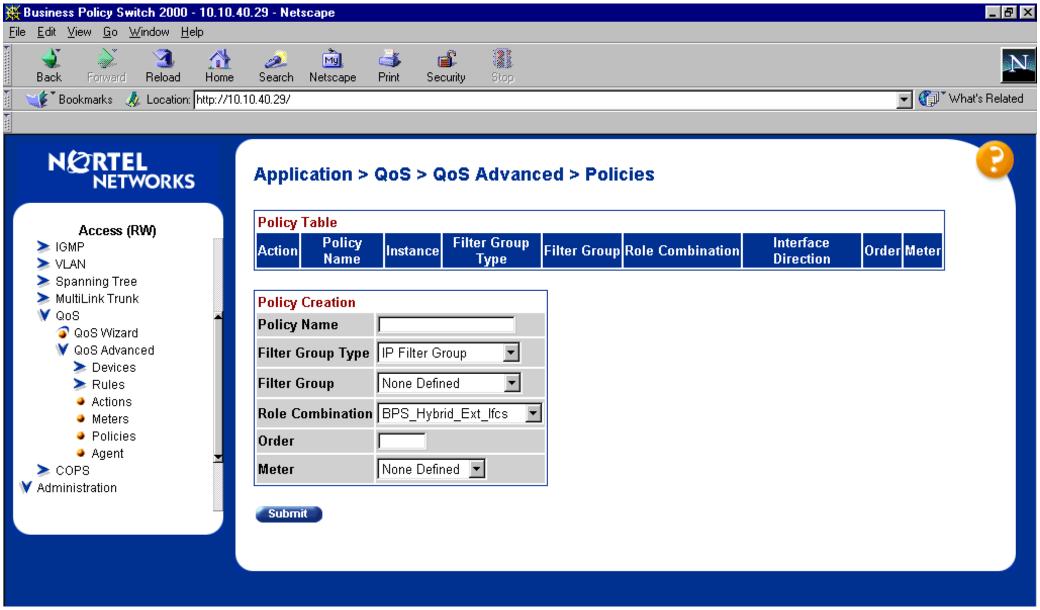
10 Choose Applications > QoS > QoS Advanced > Devices > Interface Configuration page to connect the desired ports to the desired filters.

11 Choose Applications > QoS > QoS Advanced > Policies.

Note: You cannot edit Policies. To change the Policy, you must first delete the current Policy and create the one you want.

The Policies page opens (Figure 2).

Figure 2 Policies page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
QoS Wizard
QoS Advanced
Devices
Rules
Actions
Meters
Policies
Agent
COPS
Administration
Submit

Application > QoS > QoS Advanced > Policies

Policy Table

Action	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Order	Meter

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	None Defined
Role Combination	BPS_Hybrid_Ext_Ifcs
Order	
Meter	None Defined

12 In the Policy Creation area, create the policy for each traffic policing filter.

Table 3 describes the fields in the Policy Creation Box, which you use to set new policies.

Table 3 Policy Creation fields

Field	**Description**
Policy Name	Enter the name for the policy you are creating.
Filter Group Type	Choose the filter group type from the list: • IP Filter Group • Layer2 Filter Group
Filter Group	Choose the name of the filter group for which you are creating the metering policy. (You named this filter group(s) using the IP Classification/Layer2 Classification page.)
Role Combination	Choose the name of the Role Combination for which you are creating the metering policy. (You named this Role Combination on the Interface Group page.)

Table 3 Policy Creation fields (continued)

Field	Description
Order	Specify the order of precedence among the filter groups.
Meter	Choose the name of the filter group for which you are creating the metering policy (You named this filter group on the Meter page.)

13 View the policies you previously created in the Policy Table.

14 Click Submit.

EAPOL-based security

This section contains the following information on EAPOL-based security:

- "Introduction," next
- "EAPOL-based security example" on page 16
- "Overview and terms" on page 17
- "EAPOL dynamic VLAN assignment" on page 19
- "Setting up the Authentication server" on page 20
- "Authentication process" on page 20
- "System requirements" on page 22
- "EAPOL-based security configuration rules" on page 23
- "RADIUS-based network security" on page 23
- "Configuring EAPOL using CI menus" on page 24
- "Configuring EAPOL using JDM" on page 28
- "Configuring EAPOL using the Web-based management system" on page 39

Introduction

The Extensible Authentication Protocol over LAN (EAPOL)-based security feature uses the EAP, as described in the IEEE Draft P802.1X, to allow you to set up network access control on internal LANs.

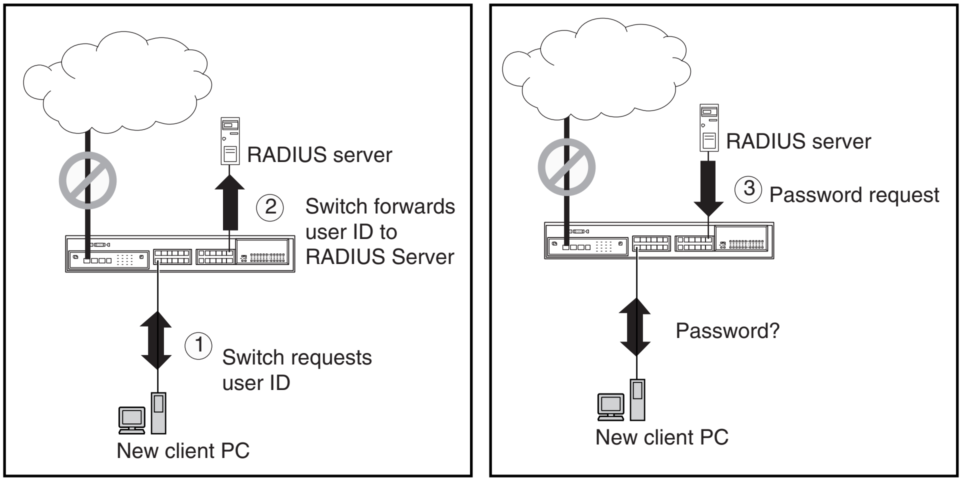
EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server (such as a RADIUS server). The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients.

EAPOL-based security example

The following example illustrates how the BPS 2000, configured with the EAPOL-based security feature, reacts to a new network connection:

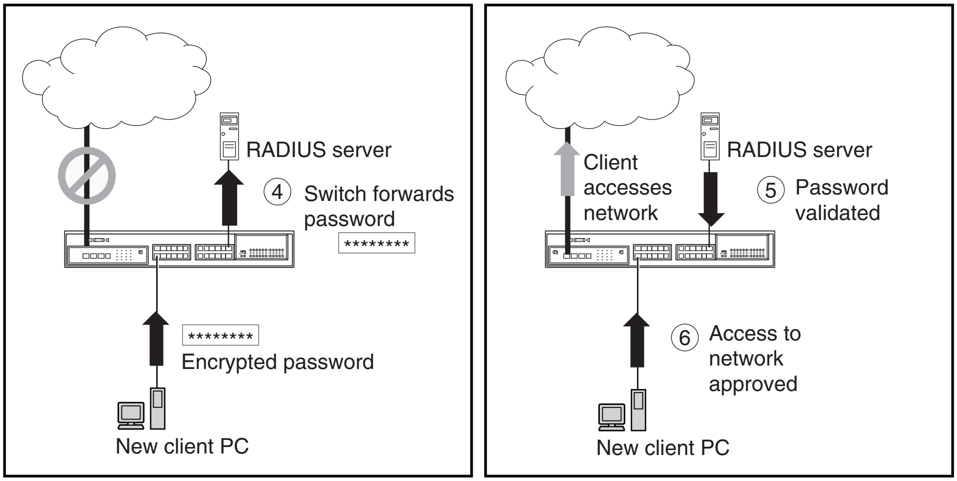
- The switch detects a new connection on one of its ports (Figure 4).
  - — The switch requests a user ID from the new client (1).
  - — EAPOL encapsulates the user ID and forwards it to the RADIUS server (2).
  - — The RADIUS server responds with a request for the user's password (3).
- The new client forwards an encrypted password to the switch, within the EAPOL packet (Figure 4).
  - — The switch relays the EAPOL packet to the RADIUS server (4).
  - — If the RADIUS server validates the password (5), the new client is allowed access to the switch and the network (6).

Figure 3 EAPOL-based security (1 of 2)


RADIUS server
② Switch forwards user ID to RADIUS Server
① Switch requests user ID
New client PC
RADIUS server
③ Password request
Password?
New client PC

EAPOL_step1

Figure 4 EAPOL-based security (2 of 2)


RADIUS server
④ Switch forwards password
****
****
Encrypted password
New client PC
Client accesses network
RADIUS server
⑤ Password validated
⑥ Access to network approved
New client PC

EAPOL_step2

Overview and terms

This section provides a detailed description of EAPOL-based security, including an overview of the components and terms used with this feature.

Some components of EAPOL-based security are:

- Supplicant—the device applying for access to the network.
- Authenticator—software with the sole purpose of authorizing a supplicant that is attached to the other end of a LAN segment.
- Authentication Server—a RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE)—a software entity associated with each port that supports the Authenticator or Supplicant functionality. In the preceding example, the Authenticator PAE resides on the switch.
- Controlled Port—any switch port with EAPOL-based security enabled.

The Authenticator communicates with the Supplicant using an encapsulation mechanism known as EAP over LANs (EAPOL).

The Authenticator PAE encapsulates the EAP message into a RADIUS packet before sending the packet to the Authentication Server. The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server by encapsulating the EAP message to make it suitable for the packet's destination.

The Authenticator determines the controlled port's operational state. After the RADIUS server notifies the Authenticator PAE about the success or failure of the authentication, it changes the controlled port's operational state accordingly.

The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch's controlled port, the controlled port's state is set to Blocking. During that time, EAP packets are processed by the authenticator.

When the Authentication server returns a "success" or "failure" message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Forwarding. Otherwise, the controlled port's state depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen.

The Operational Traffic Control field can have one of the following two values:

- Incoming and Outgoing—If the controlled port is unauthorized, frames are not transmitted through the port; all frames received on the controlled port are discarded. The controlled port's state is set to Blocking.
- Incoming—If the controlled port is unauthorized, frames received on the port are discarded, but the transmit frames are forwarded through the port.

EAPOL dynamic VLAN assignment

If EAPOL-based security is enabled on a port, and then the port is authorized, the EAPOL feature dynamically changes the port's VLAN configuration according to preconfigured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_id) in the Authentication server.

The following VLAN configuration values are affected:

- Port Membership
- PVID
- Port Priority

When the EAPOL-based security is disabled on a port that was previously authorized, the port's VLAN configuration values are restored directly from the switch's non-volatile random access memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are **not** stored in the switch's NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPOL; however, aware that the values you configure are not stored in NVRAM.
- When EAPOL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.

Setting up the Authentication server

This section describes how to set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. The Authentication server allows you to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that has been configured for EAPOL authentication, the Authentication server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication server.

To set up the Authentication server, set the following “Return List” attributes for all user configurations (refer to your Authentication server documentation):

- VLAN membership attributes
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes
  - Vendor Id: value 562, Nortel Networks vendor Id
  - Attribute Number: value 1, Port Priority
  - Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

Authentication process

The flowcharts shown in Figure 5 and Figure 6 describe the authentication process.

Figure 5 Authenticaton process flowchart (1 of 2)

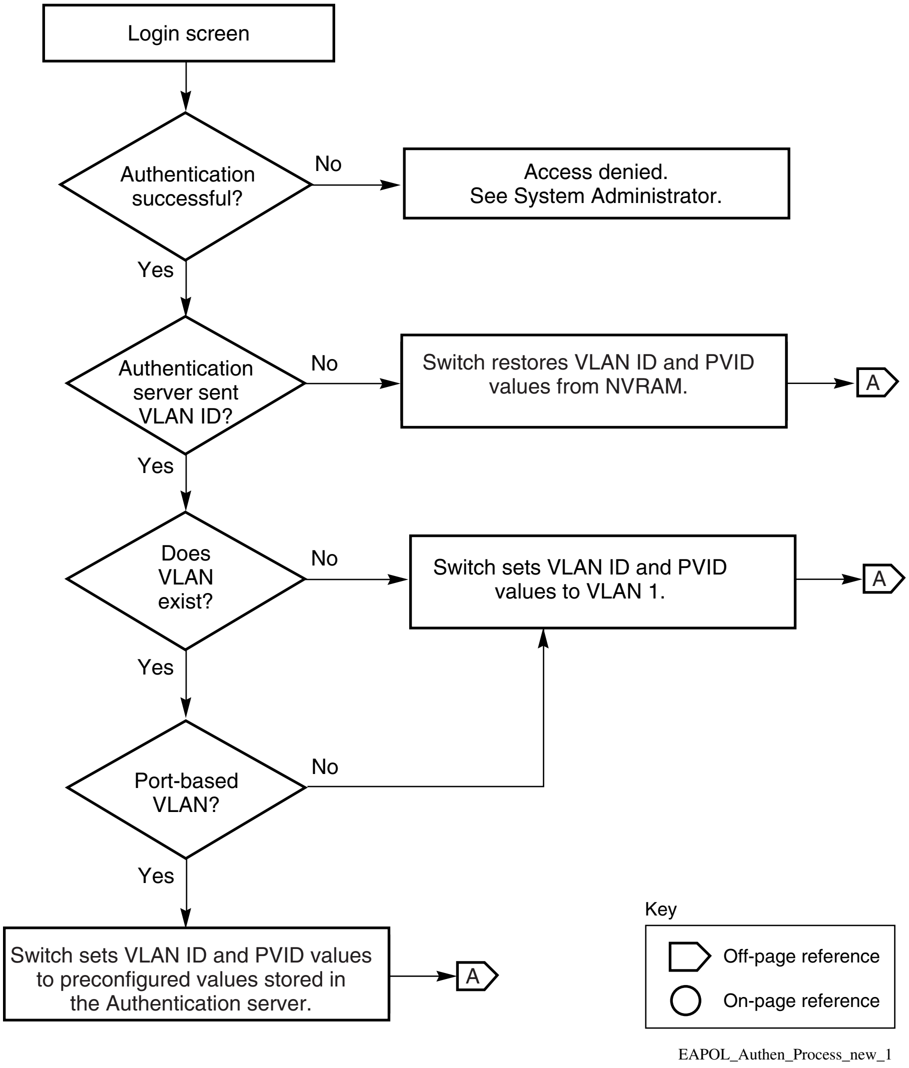
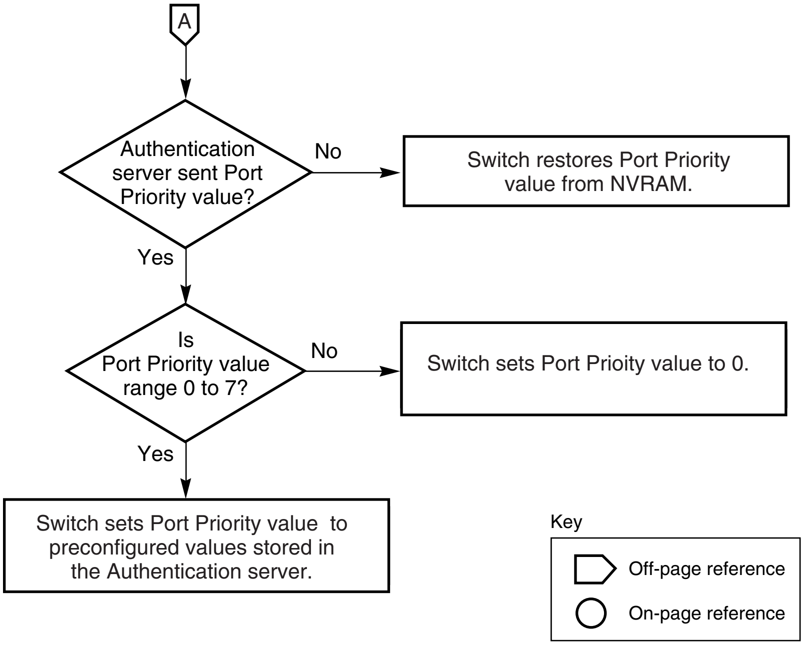

Login screen
Authentication successful?
No
Access denied. See System Administrator.
Yes
Authentication server sent VLAN ID?
No
Switch restores VLAN ID and PVID values from NVRAM.
A
Yes
Does VLAN exist?
No
Switch sets VLAN ID and PVID values to VLAN 1.
A
Yes
Port-based VLAN?
No
Yes
Switch sets VLAN ID and PVID values to preconfigured values stored in the Authentication server.
A
Key
Off-page reference
On-page reference
EAPOL_Authen_Process_new_1

Figure 6 Authenticaton process flowchart (2 of 2)


A
Authentication server sent Port Priority value?
No
Switch restores Port Priority value from NVRAM.
Yes
Is Port Priority value range 0 to 7?
No
Switch sets Port Prioity value to 0.
Yes
Switch sets Port Priority value to preconfigured values stored in the Authentication server.
Key
Off-page reference
On-page reference

EAPOL_Authen_Process_new_2

System requirements

The following are minimum system requirements for the EAPOL-based security feature:

- At least one of the following supported switches:
  - BayStack 350/410-24T/450 switch (software version V4.0, or later)
  - Business Policy Switch 2000 (software version V1.1, or later)
- RADIUS server (Microsoft* Windows* XP Server)
- Client software that supports EAPOL (Microsoft Windows XP Client)

You must configure your BayStack 350/410-24T/450 switches and BPS 2000 for port-based VLANs and EAPOL security. (For information on configuring these switches, refer to the documents shipped with the switch.)

You must also specify the Microsoft 2001 IAS server (or any generic RADIUS server that supports EAP) as the primary RADIUS server for these devices.

EAPOL-based security configuration rules

The following configuration rules apply to your BPS 2000 when using EAPOL-based security:

- Before configuring your switch, you must configure the Primary RADIUS Server and Shared Secret fields.
- You cannot configure EAPOL-based security on ports that are currently configured for:
  - Shared segments
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - Port mirroring
- You can connect only a single client on each port that is configured for EAPOL-based security. (If you attempt to add additional ports to a port, that port goes to Blocking mode.)

RADIUS-based network security

The Remote Authentication Dial-In User Services (RADIUS)-based security feature allows you to set up network access control, using the RADIUS security protocol.

The feature uses the RADIUS protocol to authenticate local console, Telnet, and EAPOL-authorized logins.

You must set up specific user accounts (user names and passwords, and Service-Type attributes) on your RADIUS server before the authentication process can be initiated.

To provide each user with appropriate levels of access to the switch, set the following username attributes on your RADIUS server:

- Read-write access—Set the Service-Type field value to Administrative.
- Read-only access—Set the Service-Type field value to NAS-Prompt.

For detailed instructions about setting up your RADIUS server, refer to your RADIUS server documentation.

Configuring EAPOL using CI menus

The EAPOL Security Configuration screen (Figure 7) allows you to selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.

Note: Before you use the EAPOL Security Configuration screen, you must configure your Primary RADIUS Server and RADIUS Shared Secret.

You will also need to set up specific user accounts on your RADIUS server:

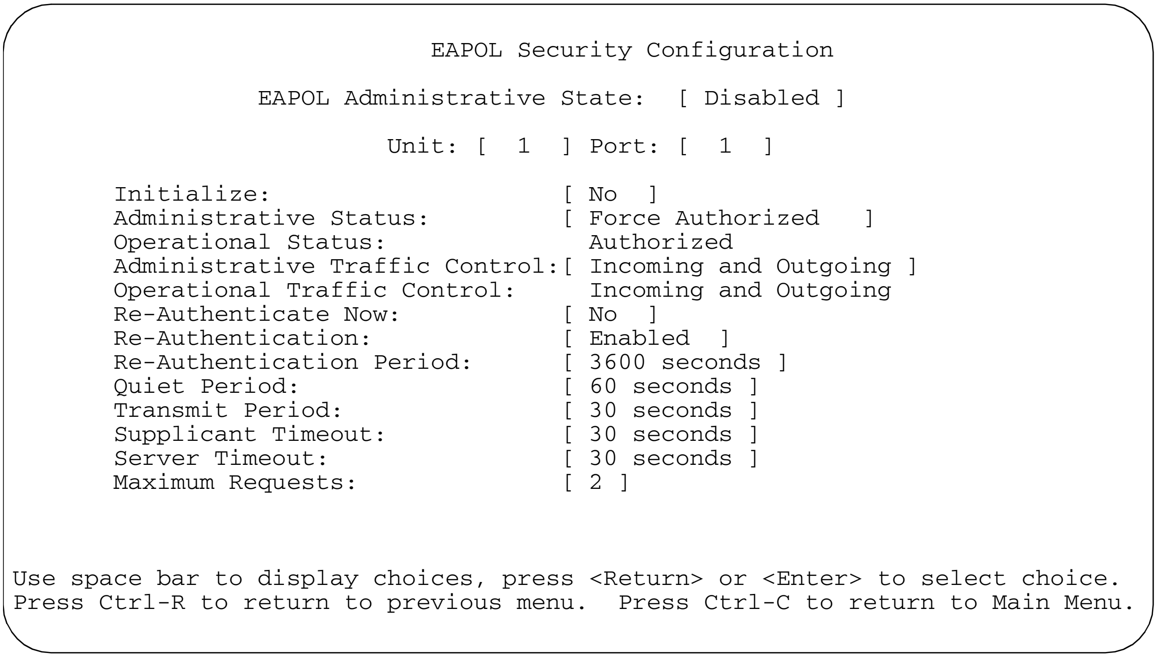
- User names
- Passwords
- VLAN IDs
- Port priority

You can set up these parameters directly on your RADIUS server. For detailed instructions about configuring your RADIUS server, refer to your RADIUS server documentation.

Note: Do not enable EAPOL security on the switch port that is connected to the RADIUS server.

➔ Choose EAPOL Security Configuration (or press e) from the Switch Configuration Menu to display the EAPOL Security Configuration screen.

Figure 7 EAPOL security configuration screen



```
                             EAPOL Security Configuration

                 EAPOL Administrative State:  [ Disabled ]

                          Unit: [  1  ] Port: [  1  ]

       Initialize:                    [ No  ]
       Administrative Status:         [ Force Authorized   ]
       Operational Status:              Authorized
       Administrative Traffic Control:[ Incoming and Outgoing ]
       Operational Traffic Control:     Incoming and Outgoing
       Re-Authenticate Now:           [ No  ]
       Re-Authentication:             [ Enabled  ]
       Re-Authentication Period:      [ 3600 seconds ]
       Quiet Period:                  [ 60 seconds ]
       Transmit Period:               [ 30 seconds ]
       Supplicant Timeout:            [ 30 seconds ]
       Server Timeout:                [ 30 seconds ]
       Maximum Requests:              [ 2 ]



Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 4 describes the EAPOL Security Configuration screen options.

Table 4 EAPOL security configuration screen options

Option	Description
EAPOL Administrative State	Allows you to enable or disable EAPOL for your switch or stack. When this field is set to Disabled (the default state), the Operational Status for all of the switch/stack ports is set to Authorized (no security restriction). Default Disabled Range Disabled, Enabled
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers. If you set this field value to All, other screen field values you modify apply to *all* stack ports. Default 1 Range 1,2,3,4,5,6,7,8,ALL

Table 4 EAPOL security configuration screen options (continued)

Option	Description
Port	Allows you to select a specified unit's (see preceding Unit field) port number to view or configure. To view or configure another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers. If you set this field value to All, other screen field values you modify apply to *all* ports for the specified unit. The All value is also useful when you want to apply modified field values to most of, but not all of, your switch's ports. For example, if you want to apply modified field values to 23 of your switch's 24 ports, it may be easier to apply the All value in the Port field, and then reconfigure the single port back to its original values. Default 1 Range 1 to 28,ALL
Initialize	Allows you to activate EAPOL authentication for the specified unit/port. Default No Range No,Yes
Administrative Status	Allows you to set the EAPOL authorization status for the specified unit/port. Default Force Authorized Range Force Authorized,Force Unauthorized,Auto • Force Authorized means the specified unit/port authorization status is *always* authorized. • Force Unauthorized means the specified unit/port authorization status is *always* Unauthorized. • Auto means the specified unit/port authorization status depends on the EAP authentication results.
Operational Status	A read-only field that shows the current authorization status for the specified unit/port. This read-only field does not appear when the Unit/Port field value is set to All. Default Authorized Range Authorized,Unauthorized
Administrative Traffic Control	Allows you to choose whether EAPOL authentication is set for incoming and outgoing traffic or for incoming traffic only. For example, if you set the specified unit/port field value to Incoming and Outgoing, and the EAPOL authentication fails, then both incoming and outgoing traffic on the specified unit/port is blocked. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only

Table 4 EAPOL security configuration screen options (continued)

Option	Description
Operational Traffic Control	A read-only field that indicates the current administrative traffic control configuration for the specified unit/port (see preceding field description). This read-only field does not appear when the Unit/Port field value is set to All. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only
Re-Authenticate Now	Allows you to activate EAPOL authentication for the specified unit/port immediately, without waiting for the Re-Authentication Period to expire. Default No Range No,Yes
Re-Authentication	Allows you to repeat EAPOL authentication for the specified unit/port according to the time interval value configured in the Re-Authentication Period field (see next field description). Default Enabled Range Enabled,Disabled
Re-Authentication Period	When the Re-Authentication field value (see preceding field) is set to Enabled, this field allows you to specify the time period between successive EAPOL authentications for the specified unit/port. Default 3600 seconds Range 1 to 604800 seconds
Quiet Period	Allows you to specify the time period between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt. Default 60 seconds Range 0 to 65535 seconds
Transmit Period	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets. Default 30 seconds Range 1 to 65535 seconds
Supplicant Timeout	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets. Default 30 seconds Range 1 to 65535 seconds
Server Timeout	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets. Default 30 seconds Range 1 to 65535 seconds

Table 4 EAPOL security configuration screen options (continued)

Option	Description
Maximum Requests	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant. Default 2 attempts Range 1 to 10 attempts

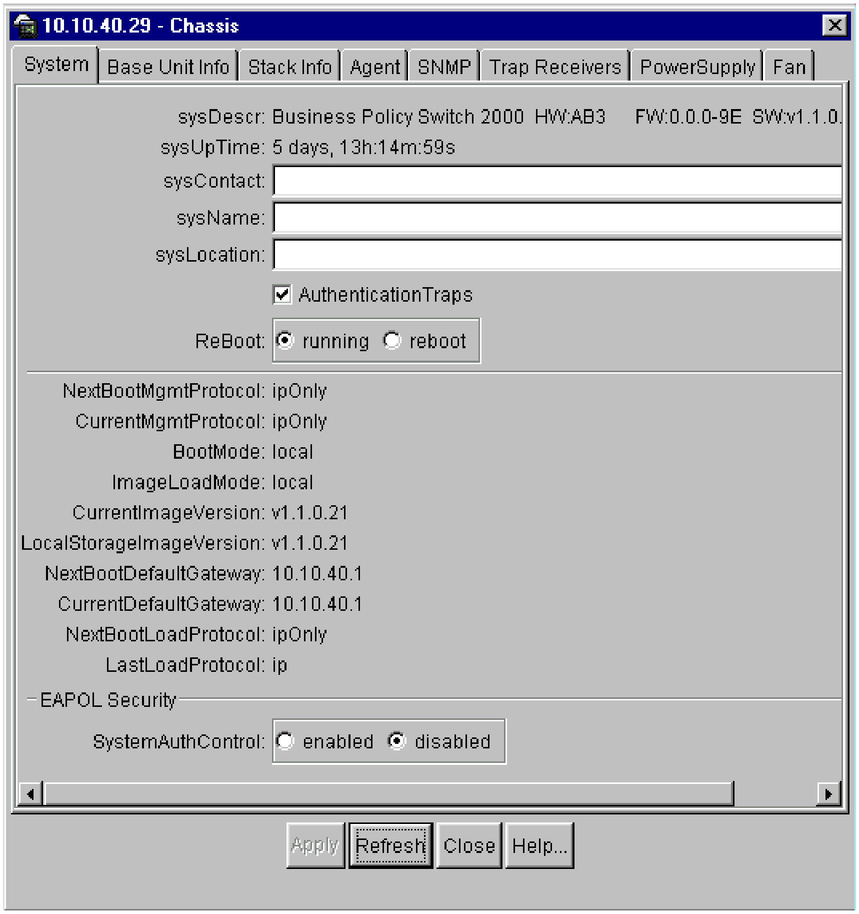
Configuring EAPOL using JDM

You can configure the BPS 2000 for EAPOL using Java Device Manager (DM). Additionally, you can view the statistics for running EAPOL and for the diagnostics.

To configure EAPOL:

1 From the Device Manager main menu, choose Edit > Chassis.

The Chassis dialog box opens, with the System tab displayed (Figure 8).



10.10.40.29 - Chassis
System
Base Unit Info
Stack Info
Agent
SNMP
Trap Receivers
PowerSupply
Fan
Apply
Refresh
Close
Help...

sysDescr: Business Policy Switch 2000 HW:AB3 FW:0.0.0-9E SW:v1.1.0.

sysUpTime: 5 days, 13h:14m:59s

sysContact:

sysName:

sysLocation:

☑ AuthenticationTraps

ReBoot: ● running ○ reboot

NextBootMgmtProtocol: ipOnly

CurrentMgmtProtocol: ipOnly

BootMode: local

ImageLoadMode: local

CurrentImageVersion: v1.1.0.21

LocalStorageImageVersion: v1.1.0.21

NextBootDefaultGateway: 10.10.40.1

CurrentDefaultGateway: 10.10.40.1

NextBootLoadProtocol: ipOnly

LastLoadProtocol: ip

EAPOL Security

SystemAuthControl: ○ enabled ● disabled

Figure 8 System tab

2. In the EAPOL Security area in the SystemAuthControl field, click enabled to enable port access control in the system.
3. Select the port you want to edit.

   Do one of the following:

   - Double-click on the selected port.
   - From the shortcut menu (right-click), choose Edit.
   - From the Device Manager main menu, choose Edit > Port.

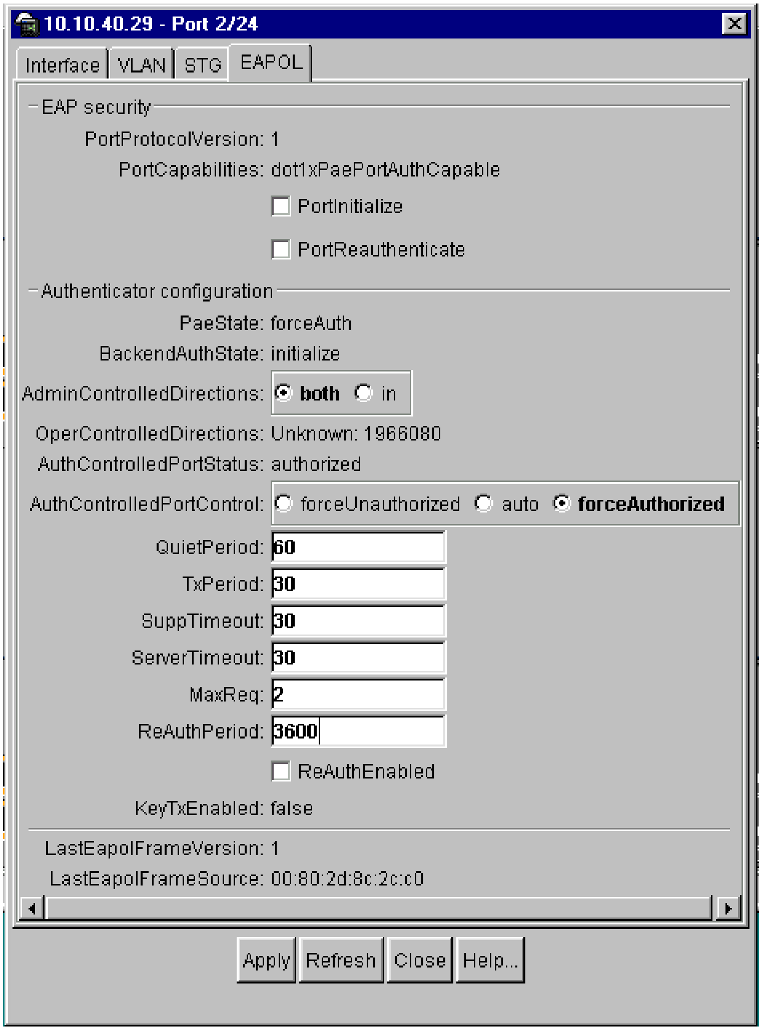
- On the toolbar, click Edit.

  The Port dialog box for a single port opens with the Interface tab displayed.

4 Click the EAPOL tab.

The EAPOL tab opens (Figure 9).

Figure 9 EAPOL tab for a single port



EAP security

PortProtocolVersion: 1

PortCapabilities: dot1xPaePortAuthCapable

☐ PortInitialize

☐ PortReauthenticate

Authenticator configuration

PaeState: forceAuth

BackendAuthState: initialize

AdminControlledDirections: ● both ○ in

OperControlledDirections: Unknown: 1966080

AuthControlledPortStatus: authorized

AuthControlledPortControl: ○ forceUnauthorized ○ auto ● forceAuthorized

QuietPeriod: 60

TxPeriod: 30

SuppTimeout: 30

ServerTimeout: 30

MaxReq: 2

ReAuthPeriod: 3600

☐ ReAuthEnabled

KeyTxEnabled: false

LastEapolFrameVersion: 1

LastEapolFrameSource: 00:80:2d:8c:2c:c0

Table 5 describes the EAPOL tab items for a single port.

Table 5 EAPOL tab items for a single port

Item	Description
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/Identity packets.
SuppTimeout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.

Table 5 EAPOL tab items for a single port (continued)

Item	Description
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

The EAPOL Stats tab shows EAPOL statistics for graphing ports.

To open the EAPOL Stats tab for graphing:

1. Select the port or ports you want to graph.

   [Ctrl]+left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

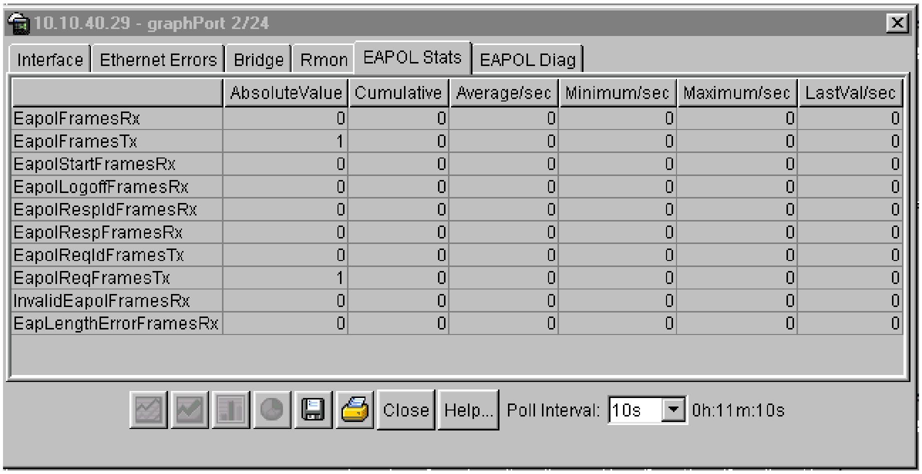
   - From the Device Manager main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The graphPort dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL Stats tab.

   The EAPOL Stats tab for graphing ports opens (Figure 10).

Figure 10 EAPOL Stats tab for graphing ports



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
EapolFramesRx	0	0	0	0	0	0
EapolFramesTx	1	0	0	0	0	0
EapolStartFramesRx	0	0	0	0	0	0
EapolLogoffFramesRx	0	0	0	0	0	0
EapolRespIdFramesRx	0	0	0	0	0	0
EapolRespFramesRx	0	0	0	0	0	0
EapolReqIdFramesTx	0	0	0	0	0	0
EapolReqFramesTx	1	0	0	0	0	0
InvalidEapolFramesRx	0	0	0	0	0	0
EapLengthErrorFramesRx	0	0	0	0	0	0

Poll Interval: 10s 0h:11m:10s

Table 6 describes the EAPOL Stats tab fields for graphing ports.

Table 6 EAPOL Stats tab fields for graphing ports

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that have been transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that have been received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that have been received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that have been transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator.

Table 6 EAPOL Stats tab fields for graphing ports (continued)

Field	**Description**
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid.

The EAPOL Diag tab shows EAPOL diagnostic information for graphing ports.

To open the EAPOL Diag tab for graphing:

1. Select the port or ports you want to graph.

   [Ctrl]+left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

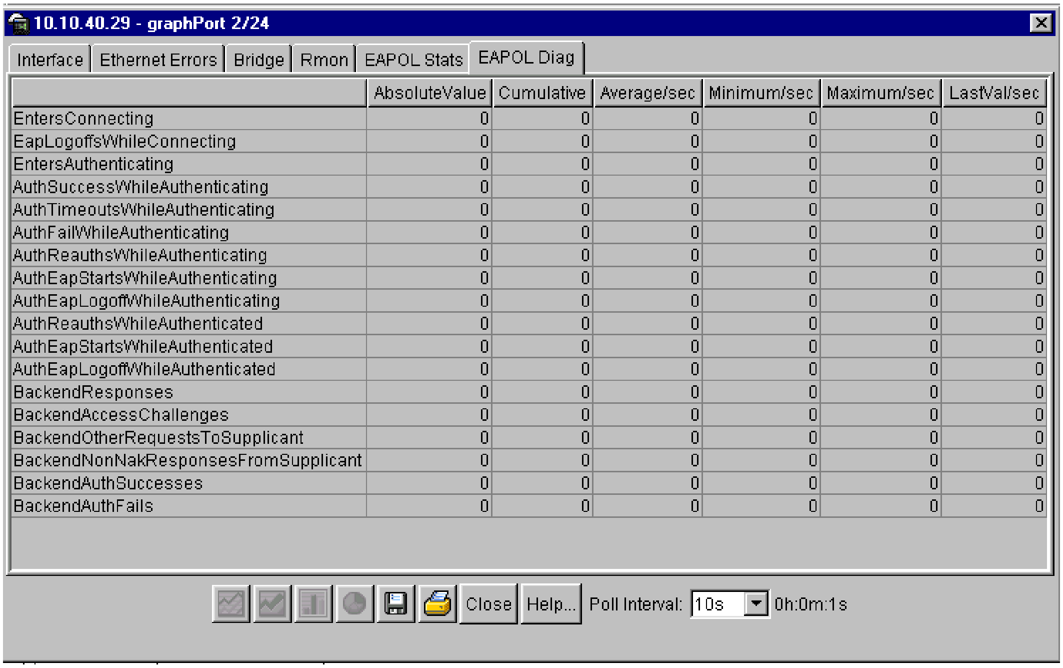
   - From the Device Manager main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The graphPort dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL Diag tab.

   The EAPOL Diag tab for graphing ports opens (Figure 11).

Figure 11 EAPOL Diag tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
EntersConnecting	0	0	0	0	0	0
EapLogoffsWhileConnecting	0	0	0	0	0	0
EntersAuthenticating	0	0	0	0	0	0
AuthSuccessWhileAuthenticating	0	0	0	0	0	0
AuthTimeoutsWhileAuthenticating	0	0	0	0	0	0
AuthFailWhileAuthenticating	0	0	0	0	0	0
AuthReauthsWhileAuthenticating	0	0	0	0	0	0
AuthEapStartsWhileAuthenticating	0	0	0	0	0	0
AuthEapLogoffWhileAuthenticating	0	0	0	0	0	0
AuthReauthsWhileAuthenticated	0	0	0	0	0	0
AuthEapStartsWhileAuthenticated	0	0	0	0	0	0
AuthEapLogoffWhileAuthenticated	0	0	0	0	0	0
BackendResponses	0	0	0	0	0	0
BackendAccessChallenges	0	0	0	0	0	0
BackendOtherRequestsToSupplicant	0	0	0	0	0	0
BackendNonNakResponsesFromSupplicant	0	0	0	0	0	0
BackendAuthSuccesses	0	0	0	0	0	0
BackendAuthFails	0	0	0	0	0	0

Poll Interval: 10s 0h:0m:1s

Table 7 describes the EAPOL Diag tab fields for graphing ports.

Table 7 EAPOL Diag tab fields for graphing ports

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/ Identity message being received from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.

Table 7 EAPOL Diag tab fields for graphing ports (continued)

Field	**Description**
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant.

Table 7 EAPOL Diag tab fields for graphing ports (continued)

Field	**Description**
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

The EAPOL tab shows EAPOL statistics for multiple ports.

To open the EAPOL tab for multiple ports:

1. Select the port or ports you want to graph.

   [Ctrl]+left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

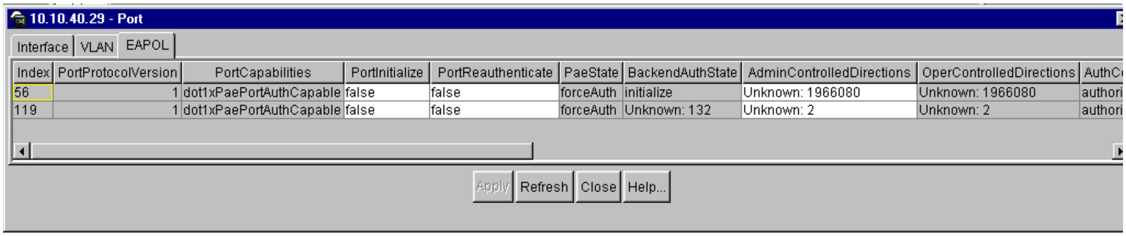
   - From the Device Manager main menu, choose Edit > Port.
   - From the shortcut menu, choose Edit.
   - On the toolbar, click Edit.

   The Port dialog box for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL tab.

   The EAPOL tab for multiple ports opens (Figure 12).

Figure 12 EAPOL tab for multiple ports



Index	PortProtocolVersion	PortCapabilities	PortInitialize	PortReauthenticate	PaeState	BackendAuthState	AdminControlledDirections	OperControlledDirections	AuthC
56	1	dot1xPaePortAuthCapable	false	false	forceAuth	initialize	Unknown: 1966080	Unknown: 1966080	authori
119	1	dot1xPaePortAuthCapable	false	false	forceAuth	Unknown: 132	Unknown: 2	Unknown: 2	authori

Table 8 describes the EAPOL tab fields for multiple ports.

Table 8 EAPOL tab fields for multiple ports

Field	Description
Index	Displays the unique value assigned to each interface.
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/Identity packets.
SuppTiemout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.

Table 8 EAPOL tab fields for multiple ports (continued)

Field	Description
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.
LastEapolFrameVersion	
LastEapolFrameSource	

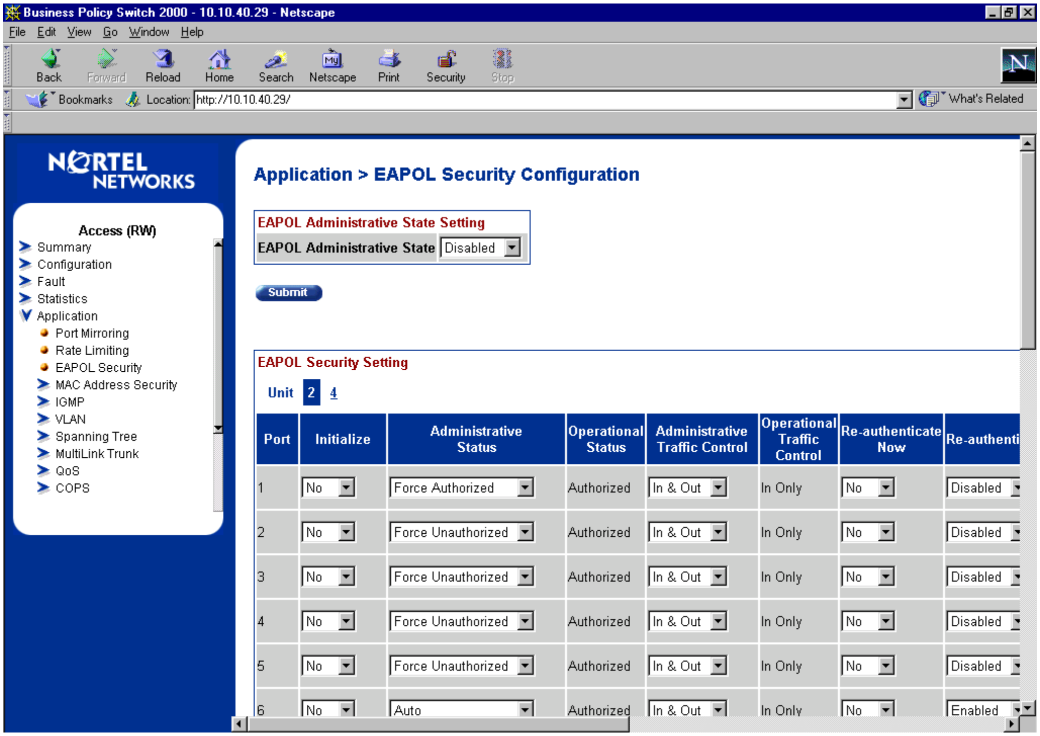
Configuring EAPOL using the Web-based management system

To configure EAPOL using the Web-based management system:

1 From the main menu of the Business Policy Switch 2000 Web-based Manager, choose Application > EAPOL Security.

The EAPOL Security Configuration page opens (Figure 13 and Figure 14). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

Figure 13 EAPOL Security Configuration page (1 of 2)



Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
COPS
Submit

Application > EAPOL Security Configuration

EAPOL Administrative State Setting

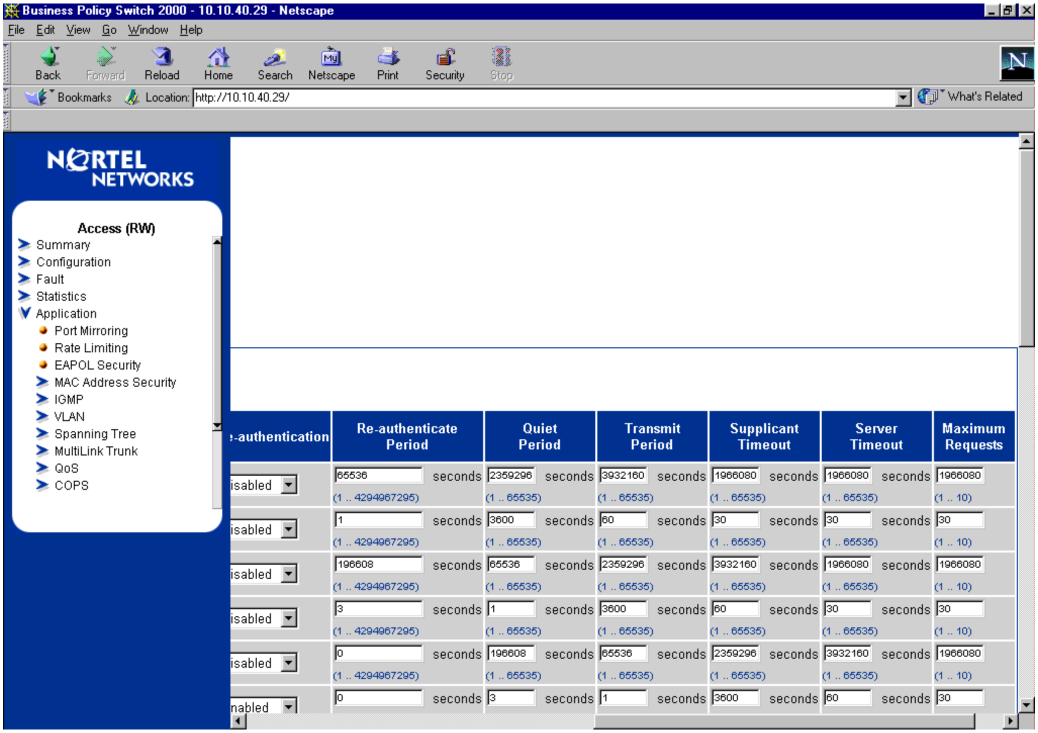
EAPOL Administrative State: Disabled

EAPOL Security Setting

Unit 2 4

Port	Initialize	Administrative Status	Operational Status	Administrative Traffic Control	Operational Traffic Control	Re-authenticate Now	Re-authenti
1	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
2	No	Force Unauthorized	Authorized	In & Out	In Only	No	Disabled
3	No	Force Unauthorized	Authorized	In & Out	In Only	No	Disabled
4	No	Force Unauthorized	Authorized	In & Out	In Only	No	Disabled
5	No	Force Unauthorized	Authorized	In & Out	In Only	No	Disabled
6	No	Auto	Authorized	In & Out	In Only	No	Enabled

Figure 14 EAPOL Security Configuration page (2 of 2)


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
COPS

-authentication	Re-authenticate Period	Quiet Period	Transmit Period	Supplicant Timeout	Server Timeout	Maximum Requests
isabled	65536 seconds (1 .. 4294967295)	2359296 seconds (1 .. 65535)	3932160 seconds (1 .. 65535)	1966080 seconds (1 .. 65535)	1966080 seconds (1 .. 65535)	1966080 (1 .. 10)
isabled	1 seconds (1 .. 4294967295)	3600 seconds (1 .. 65535)	60 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 (1 .. 10)
isabled	196608 seconds (1 .. 4294967295)	65536 seconds (1 .. 65535)	2359296 seconds (1 .. 65535)	3932160 seconds (1 .. 65535)	1966080 seconds (1 .. 65535)	1966080 (1 .. 10)
isabled	3 seconds (1 .. 4294967295)	1 seconds (1 .. 65535)	3600 seconds (1 .. 65535)	60 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 (1 .. 10)
isabled	0 seconds (1 .. 4294967295)	196608 seconds (1 .. 65535)	65536 seconds (1 .. 65535)	2359296 seconds (1 .. 65535)	3932160 seconds (1 .. 65535)	1966080 (1 .. 10)
nabled	0 seconds	3 seconds	1 seconds	3600 seconds	60 seconds	30

Table 9 describes the fields on the EAPOL Security Configuration page.

Table 9 EAPOL Security Configuration page fields

Field	**Description**
EAPOL Administrative State	Enables or disables EAPOL-based security.
Port	Displays the port number.
Initialize	Choosing Yes from the list activates EAPOL state on this port.
Administrative Status	Allows you to set the EAPOL authorization status for the specified unit/port: • Force Unauthorized—Always unauthorized • Auto—Status depends on EAP authentication results • Force Authorized—Always authorized
Operational Status	Displays the current authorization status.

Table 9 EAPOL Security Configuration page fields (continued)

Field	**Description**
Administrative Traffic Control	Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only: • In & Out—Incoming and outgoing traffic • In Only—Incoming traffic only
Operational Traffic Control	Displays the current administrative traffic control setting.
Re-authenticate Now	Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire: • Yes—Re-authenticate now • No—Wait for the period to expire
Re-authentication	Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field by choosing Enabled or Disabled.
Re-authentication Period	With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications. You can set this field between 1 and 604800 seconds.
Quiet Period	Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt. You can set this field between 0 and 65535 seconds.
Transmit Period	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets. You can set this field between 1 and 65535 seconds.
Supplicant Timeout	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets. You can set this field between 1 and 65535 seconds.
Server Timeout	Allows you to specify how long the switch wits for the RADIUS server to respond to all EAP packets. You can set this field between 1 and 65535 seconds.
Maximum Requests	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant. You can set this field between 1 and 10 attempts.

2 After making any changes to the EAPOL Security Configuration page, click Submit.

Support for the GBIC MDA

The BPS 2000 software version 1.1 supports the Gigabit Interface Connector (GBIC) MDA. The MDA, BayStack 450-1GBIC MDA, provides only two priority queues.

The BayStack 450-1GBIC MDA supports the following GBICs:

- 1000BASE-SX—This GBIC uses shortwave 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable.
- 1000BASE-LX—This GBIC uses longwave 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable.
- 1000BASE-XD—This GBIC uses single mode fiber to connect devices over distances up to 50 km (or 31 mi), depending on the quality of the cable.
- 1000BASE-ZX—This GBIC uses single mode fiber to connect devices over distances up to 70 km (or 43 mi), depending on the quality of the cable. The ports on this GBIC operate only in full-duplex mode.

For more information on this MDA as well as installation and cabling instructions, refer to *Installing Media Dependent Adapters (MDAs),* which is displayed on the Web site described in "Related publications."

Automatic PVID

This section contains the following information on Automatic PVIDs:

- "Introduction," next
- "PVID/VLAN association example" on page 44
- "Configuring Automatic PVID using CI menus" on page 45
- "Configuring Automatic PVID using the Web-based management system" on page 49

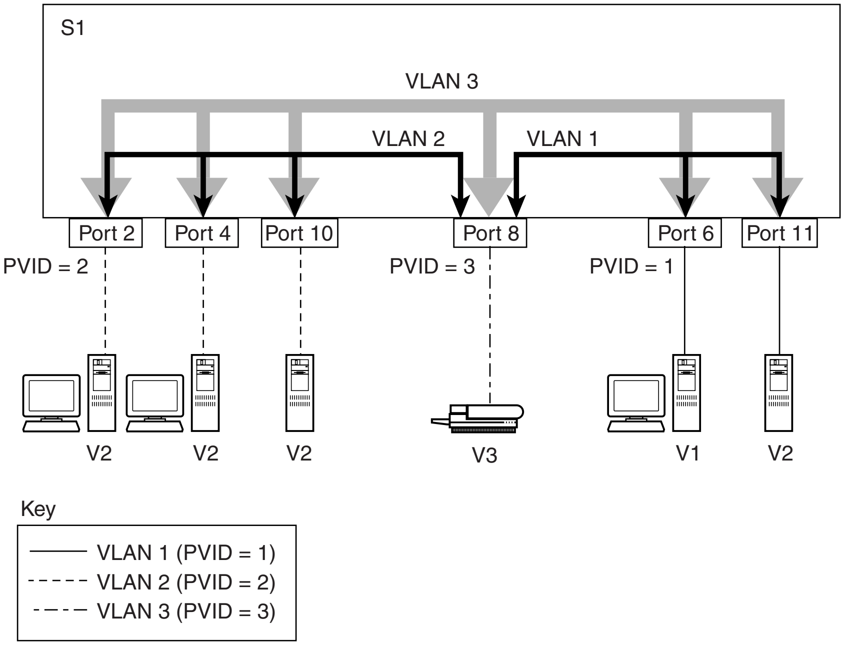
Introduction

After setting a VLAN ID in earlier software releases, the user had to also manually configure the port VLAN ID (PVID). In the software version 1.1, automatic PVID automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value. The default setting for AutoPVID is Off; you must enable this feature.

PVID/VLAN association example

For example, to create a broadcast domain for each VLAN shown in Figure 15, configure each VLAN with a port membership and each port with the appropriate PVID/VLAN association:

Figure 15 VLAN broadcast domains within the switch


S1
VLAN 3
VLAN 2
VLAN 1
Port 2
Port 4
Port 10
Port 8
Port 6
Port 11
PVID = 2
PVID = 3
PVID = 1
V2
V2
V2
V3
V1
V2
Key
VLAN 1 (PVID = 1)
VLAN 2 (PVID = 2)
VLAN 3 (PVID = 3)

BS45019A

In Figure 15 the ports have the following PVID/VLAN associations:

- Ports 8, 6, and 11 are untagged members of VLAN 1.

  The PVID/VLAN association for ports 6 and 11 is: PVID = 1.
- Ports 2, 4, 10, and 8 are untagged members of VLAN 2.

  The PVID/VLAN association for ports 2, 4, and 10 is: PVID = 2.
- Ports 2, 4, 10, 8, 6, and 11 are untagged members of VLAN 3.

  The PVID/VLAN association for port 8 is: PVID = 3.

Configuring Automatic PVID using CI menus

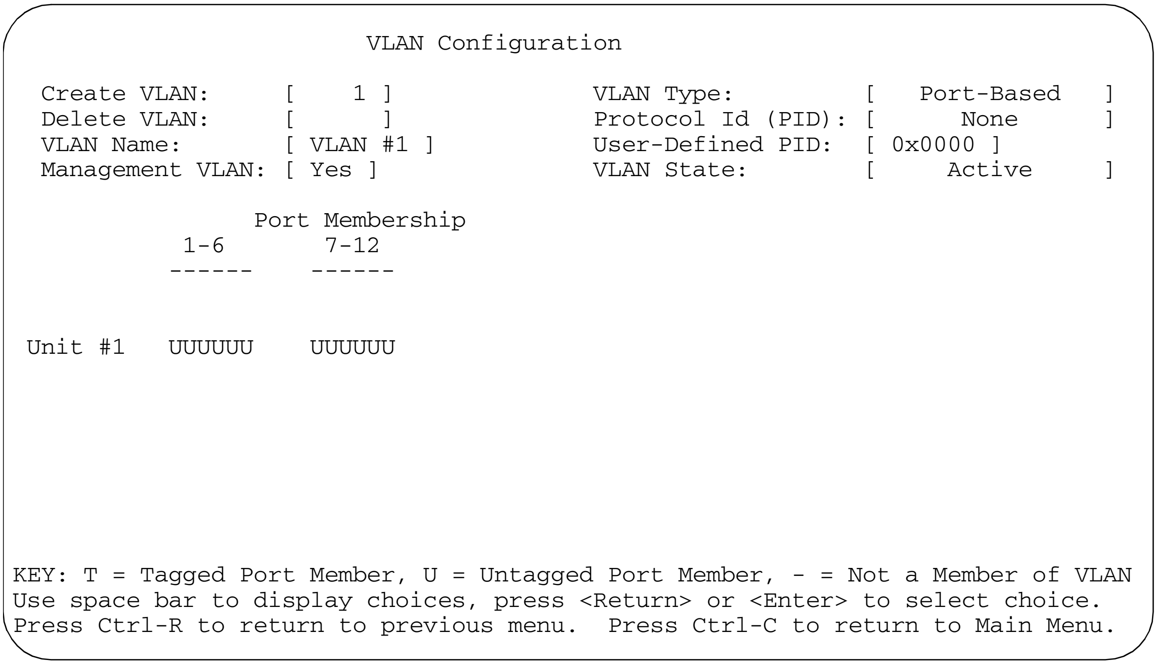
The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in Figure 15.

To configure the VLAN port membership for VLAN 1:

1. Select Switch Configuration from the Main Menu (or press w).
2. From the Switch Configuration Menu, select VLAN Configuration (or press v).
3. From the VLAN Configuration Menu select VLAN Configuration (or press v).

   The default VLAN Configuration screen opens (Figure 16):

Figure 16 Default VLAN configuration screen example



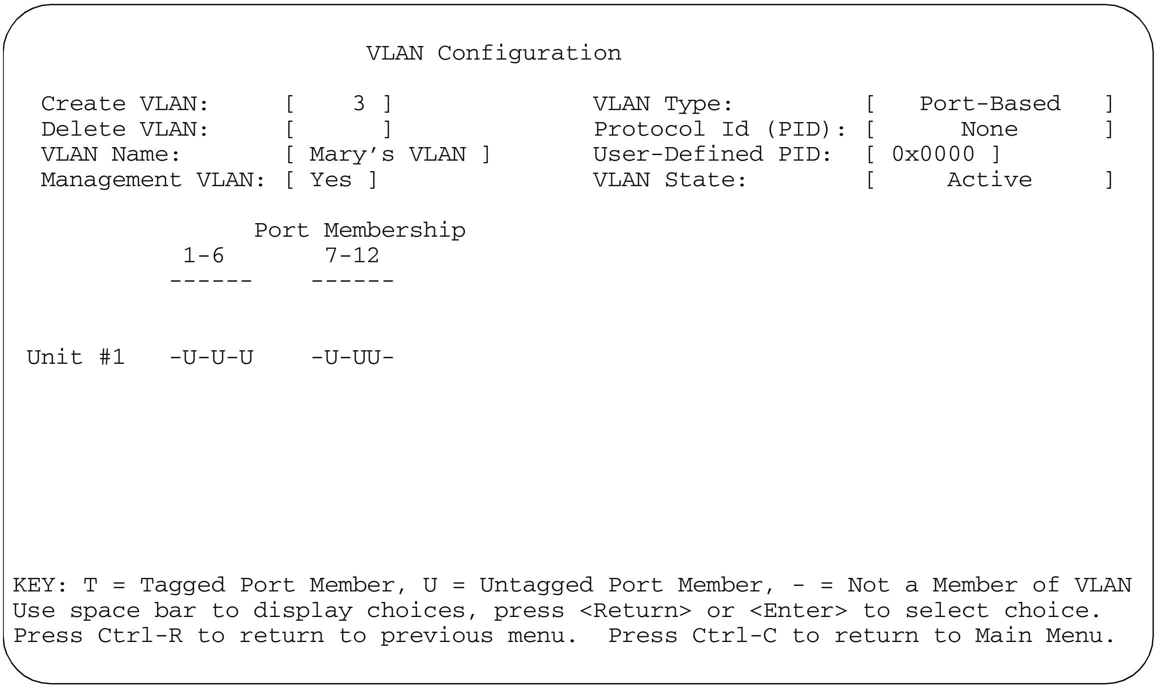
```
                           VLAN Configuration

  Create VLAN:      [    1 ]                 VLAN Type:           [   Port-Based    ]
  Delete VLAN:      [      ]                 Protocol Id (PID): [      None       ]
  VLAN Name:        [ VLAN #1 ]              User-Defined PID:  [ 0x0000 ]
  Management VLAN: [ Yes ]                   VLAN State:          [     Active      ]

                   Port Membership
              1-6        7-12
             ------     ------


 Unit #1    UUUUUU     UUUUUU







KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of VLAN
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

The VLAN Configuration screen settings shown in Figure 16 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 17 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 15 (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 15.

Figure 17 VLAN configuration screen example



```
                       VLAN Configuration

  Create VLAN:      [    3 ]            VLAN Type:          [   Port-Based   ]
  Delete VLAN:      [      ]            Protocol Id (PID):  [      None      ]
  VLAN Name:        [ Mary's VLAN ]     User-Defined PID:   [ 0x0000 ]
  Management VLAN:  [ Yes ]             VLAN State:         [     Active     ]

               Port Membership
          1-6       7-12
         ------    ------


 Unit #1   -U-U-U    -U-UU-







KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of VLAN
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

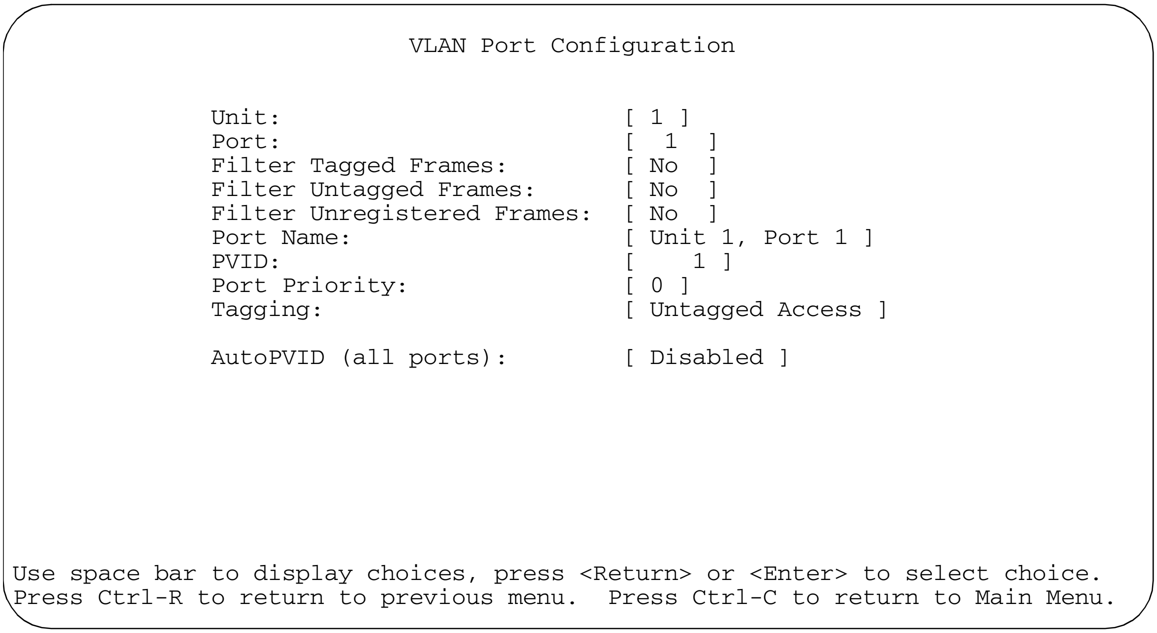
To configure the PVID (port VLAN identifier) for Port 8:

1. From the VLAN Configuration screen, press [Ctrl]-R to return to the VLAN Configuration Menu.
2. From the VLAN Configuration Menu, select VLAN Port Configuration (or press c).

   The default VLAN Port Configuration screen opens (Figure 18).

The VLAN Port Configuration screen settings shown in Figure 18 are default settings.

Figure 18 Default VLAN port configuration screen example

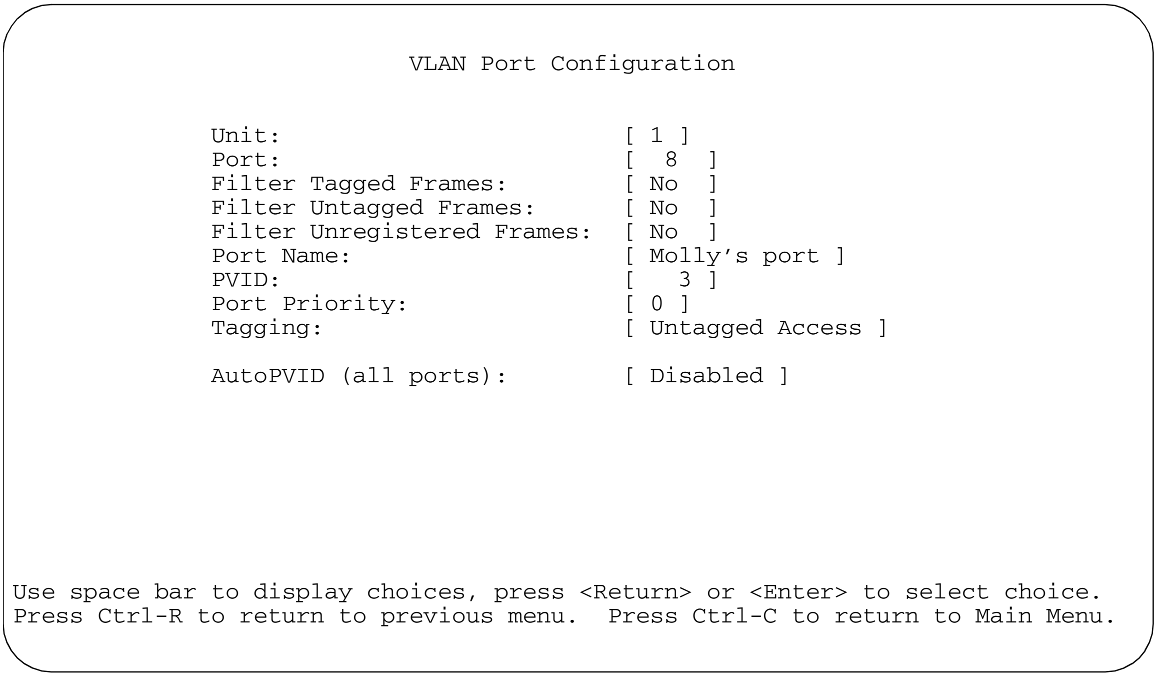


```
                           VLAN Port Configuration


              Unit:                          [ 1 ]
              Port:                          [  1  ]
              Filter Tagged Frames:          [ No  ]
              Filter Untagged Frames:        [ No  ]
              Filter Unregistered Frames:    [ No  ]
              Port Name:                     [ Unit 1, Port 1 ]
              PVID:                          [    1 ]
              Port Priority:                 [ 0 ]
              Tagging:                       [ Untagged Access ]

              AutoPVID (all ports):          [ Disabled ]








Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 19 shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8 (as shown in Figure 15). The Port Name field is optional.

As shown in Figure 19, the PVID/VLAN association for VLAN 3 is now PVID = 3.

Figure 19 VLAN port configuration screen example



```
                       VLAN Port Configuration


            Unit:                        [ 1 ]
            Port:                        [  8  ]
            Filter Tagged Frames:        [ No  ]
            Filter Untagged Frames:      [ No  ]
            Filter Unregistered Frames:  [ No  ]
            Port Name:                   [ Molly's port ]
            PVID:                        [   3 ]
            Port Priority:               [ 0 ]
            Tagging:                     [ Untagged Access ]

            AutoPVID (all ports):        [ Disabled ]







Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

The preceding example explains how to manually configure the PVID/VLAN association to PVID 3. However, if you set the AutoPVID field value to Enabled before creating the VLAN port memberships, the PVID/VLAN association is automatically assigned a value that is associated with the VLAN number you create.

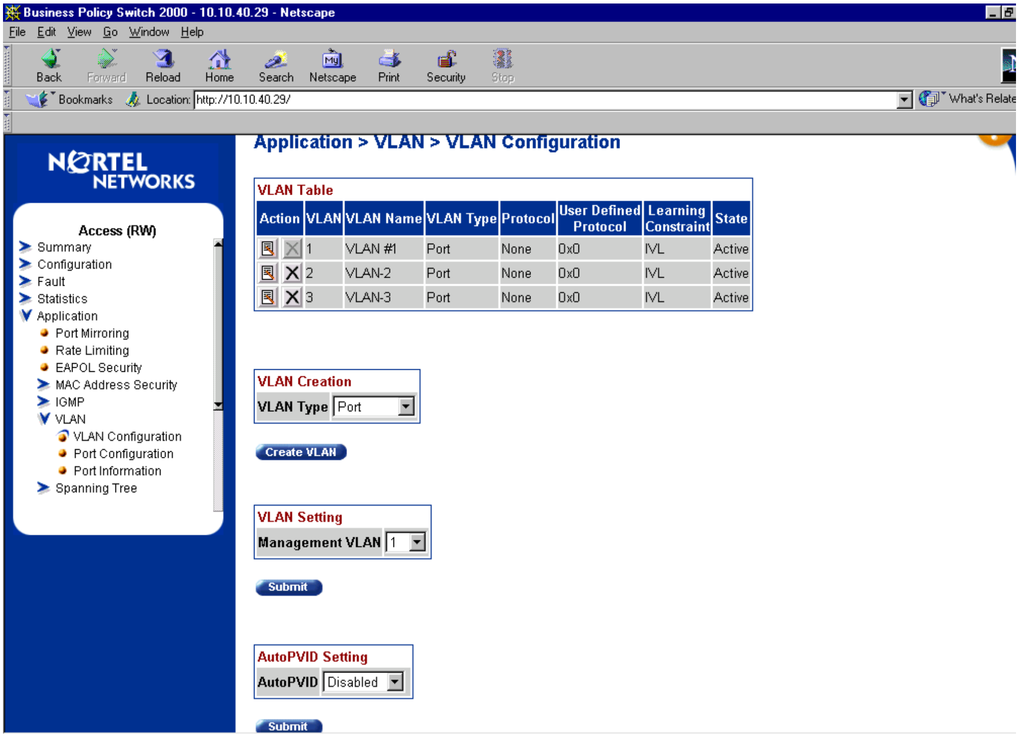
Configuring Automatic PVID using the Web-based management system

To configure AutoPVID using the Web-based management system:

1. From the main menu of the Business Policy Switch 2000 Web-based Manager, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 20).

Figure 20 VLAN Configuration page



Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
VLAN Configuration
Port Configuration
Port Information
Spanning Tree
Create VLAN
Submit
Submit

Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
	1	VLAN #1	Port	None	0x0	IVL	Active
	2	VLAN-2	Port	None	0x0	IVL	Active
	3	VLAN-3	Port	None	0x0	IVL	Active

VLAN Creation

VLAN Type: Port

VLAN Setting

Management VLAN: 1

AutoPVID Setting

AutoPVID: Disabled

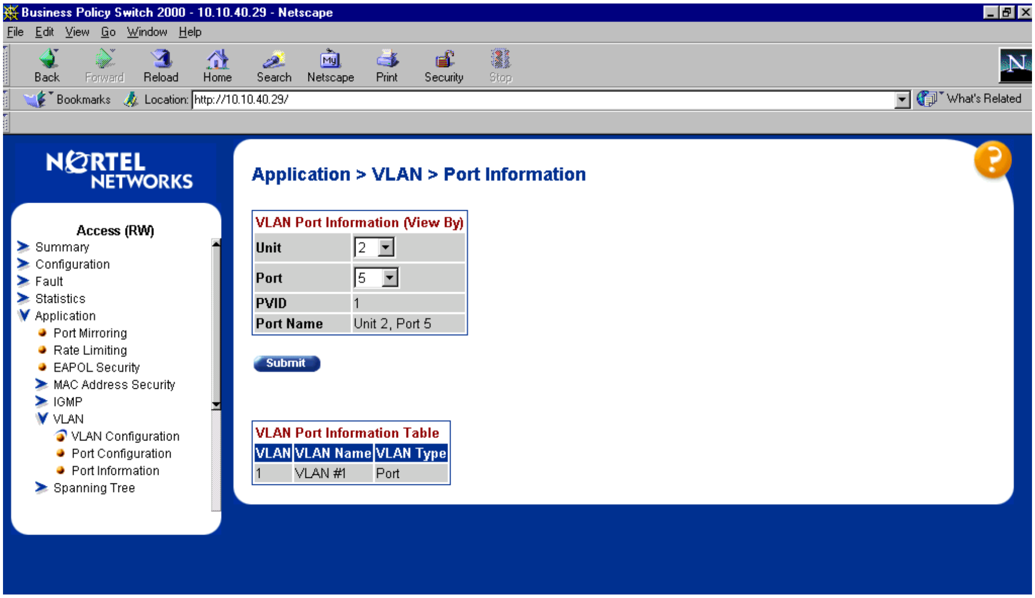
2 Choose Enabled from the AutoPVID list in the AutoPVID Setting area.

3 Click Submit.

4 To view the PVID value by port, choose Application > VLAN > Port Information.

The Port Information page opens (Figure 21), and displays the PVID value for the selected port.

Figure 21 Port Information page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
VLAN Configuration
Port Configuration
Port Information
Spanning Tree
Submit

Application > VLAN > Port Information

VLAN Port Information (View By)

Unit	2
Port	5
PVID	1
Port Name	Unit 2, Port 5

VLAN Port Information Table

VLAN	VLAN Name	VLAN Type
1	VLAN #1	Port

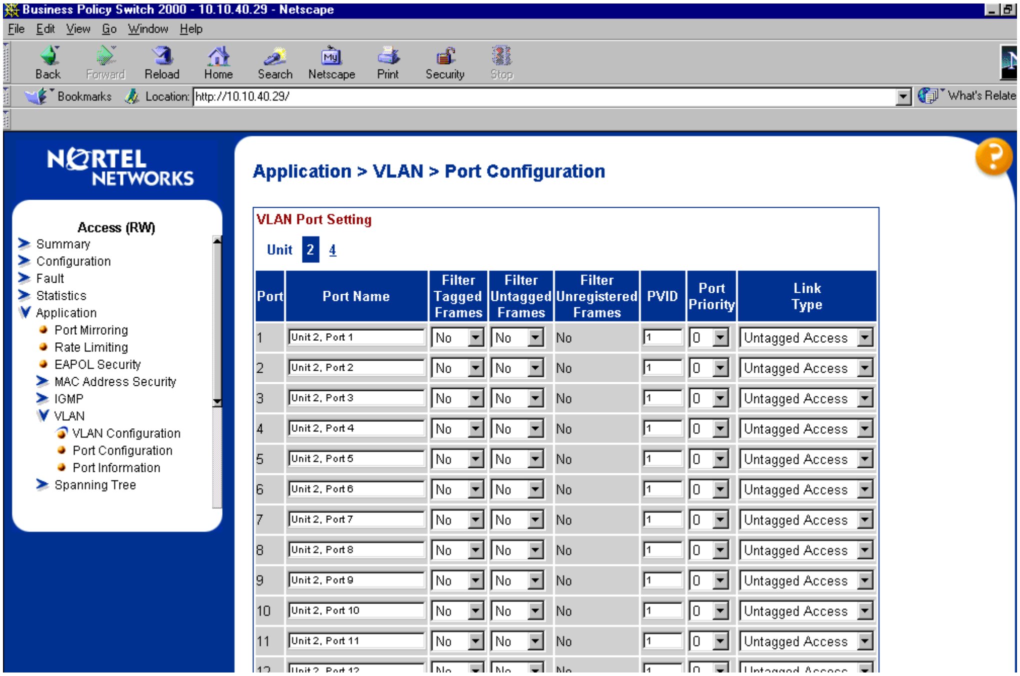
a To view the information for other ports, choose desired port from the lists by Unit and Port.

b Click Submit.

5 To manually change the PVID value of a port, choose Application > VLAN > Port Configuration.

The Port Configuration page opens (Figure 22).

Figure 22 Port Configuration page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
VLAN Configuration
Port Configuration
Port Information
Spanning Tree

Application > VLAN > Port Configuration

VLAN Port Setting

Unit 2 4

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Link Type
1	Unit 2, Port 1	No	No	No	1	0	Untagged Access
2	Unit 2, Port 2	No	No	No	1	0	Untagged Access
3	Unit 2, Port 3	No	No	No	1	0	Untagged Access
4	Unit 2, Port 4	No	No	No	1	0	Untagged Access
5	Unit 2, Port 5	No	No	No	1	0	Untagged Access
6	Unit 2, Port 6	No	No	No	1	0	Untagged Access
7	Unit 2, Port 7	No	No	No	1	0	Untagged Access
8	Unit 2, Port 8	No	No	No	1	0	Untagged Access
9	Unit 2, Port 9	No	No	No	1	0	Untagged Access
10	Unit 2, Port 10	No	No	No	1	0	Untagged Access
11	Unit 2, Port 11	No	No	No	1	0	Untagged Access
12	Unit 2, Port 12	No	No	No	1	0	Untagged Access

a Enter the PVID value you want in the box for that port.

b Click Submit.

Tabular port statistics

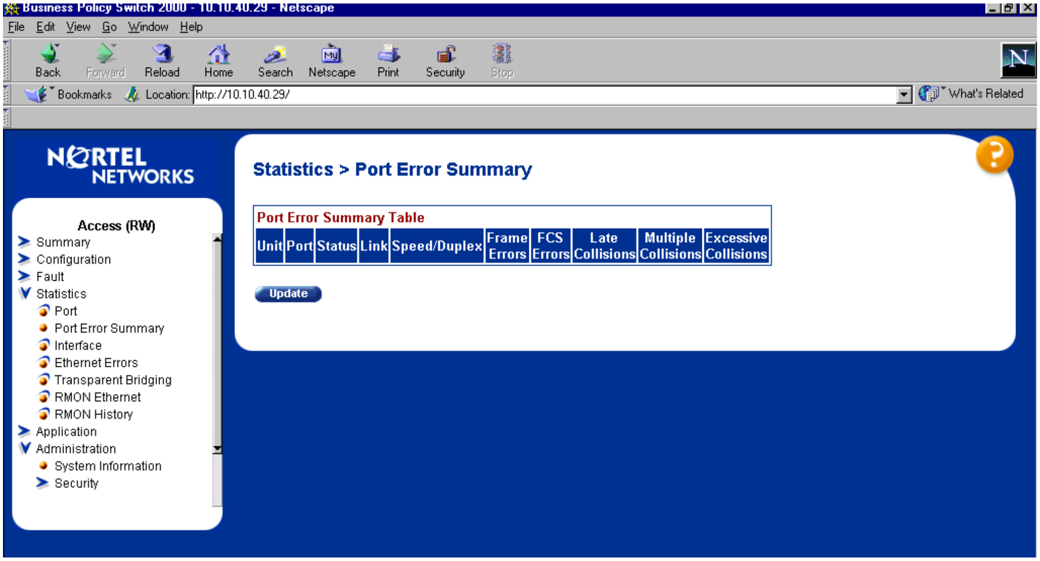
With software version 1.1, you can view all ports in the entire stack hat have an error. If a particular port has no errors, it will not be displayed.

To view a summary of the port errors for the BPS 2000:

1 From the main menu of the Business Policy Switch 2000 Web-based management system, choose Statistics > Port Error Summary.

The Port Error Summary page opens (Figure 23).

Figure 23 Port Error Summary page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Port
Port Error Summary
Interface
Ethernet Errors
Transparent Bridging
RMON Ethernet
RMON History
Application
Administration
System Information
Security
Statistics > Port Error Summary
Update

Port Error Summary Table

Unit	Port	Status	Link	Speed/Duplex	Frame Errors	FCS Errors	Late Collisions	Multiple Collisions	Excessive Collisions

Table 10 describes the read-only information displayed in the Port Error Summary Table.

Table 10 Port Error Summary Table fields

Item	Description
Unit	Displays the unit number in the stack.
Port	Displays the port number of the unit.
Status	Displays the status of the port (Enabled/Disabled).

Table 10 Port Error Summary Table fields (continued)

Item	Description
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
Frame Errors	Displays the number of frame errors received on this port.
FCS errors	Displays the number of frame check sequence (FCS) errors received on this port.
Late Collisions	Displays the number of late collisions errors received on this port.
Multiple Collisions	Displays the number of multiple collisions errors received on this port.
Excessive Collisions	Displays the number of excessive collisions errors received on this port.

2 To view the latest port statistics, click the Update button at the bottom of the page.

Ability to ping

With software version 1.1, you can ping from a BPS 2000. This ability greatly enhances the ease of network management.

Improved STP Fast Learning Mode

A front BPS 2000 port set for Fast Learning Mode for the Spanning Tree Protocol (STP) is improved in version 1.1 of BPS 2000 software. The port can forward data immediately, as soon as it detects that the link is on.

BootP menu item for a stack of only BPS 2000 switches

In a stack consisting only of BPS 2000 switches, you can perform BootP using the MAC address of the base unit.

You must use the console interface (CI) menus to choose this option.

To set this feature:

1. Open the Main Menu of the BPS 2000.
2. Choose Switch Configuration > Stack Operational Mode.

   The menu contains the following new option:

   ```
   Stack BootP Mac Address Type: [  Stack Mac Address   ]

                                 [Base Unit Mac Address]
   ```

   Toggle between the two choices using the space bar.
3. Press Enter.

The chosen setting is saved even when the stack is reset, and the default setting is Stack Mac Address. You cannot choose Base Unit Mac Address when the Stack Operational Mode is Hybrid Stack. If you do so, you see the following error message:

```
BootP with Base Unit Mac Address is not supported in Hybrid
Stack.
```

Additional Web-based management operation

BPS 2000 software version 1.1 offers the following enhancements to the Web-based management system:

- "Access to the Web-based management system using JDM," next
- "Additional Java security" on page 57
- "MAC address-based security" on page 57

Access to the Web-based management system using JDM

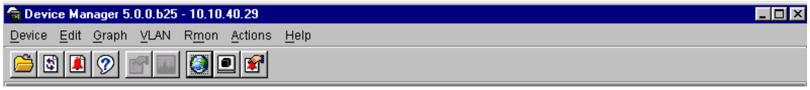
You can access the Web-based management system using JDM.

To access the Web-based management system using JDM:

➔ Do one of the following:

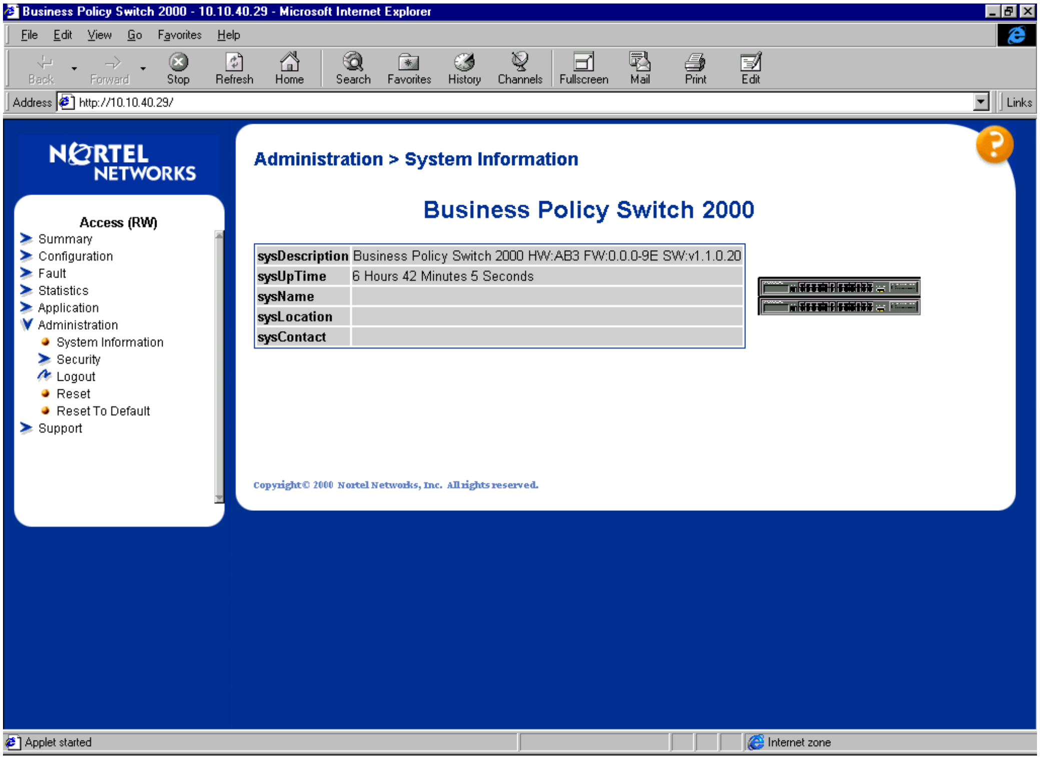
- Choose Actions > Open Home Page.
- Click the globe icon shown on the toolbar (Figure 24).

Figure 24 JDM toolbar


Device Manager 5.0.0.b25 - 10.10.40.29
Device
Edit
Graph
VLAN
Rmon
Actions
Help

The System Information opens (Figure 25).

Figure 25 System Information page


Business Policy Switch 2000 - 10.10.40.29 - Microsoft Internet Explorer
File
Edit
View
Go
Favorites
Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Channels
Fullscreen
Mail
Print
Edit
Address
http://10.10.40.29/
Links
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Administration
System Information
Security
Logout
Reset
Reset To Default
Support
Applet started
Internet zone

Administration > System Information

Business Policy Switch 2000

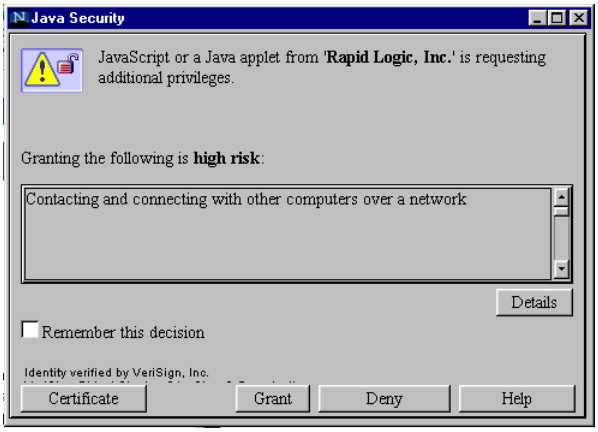
sysDescription	Business Policy Switch 2000 HW:AB3 FW:0.0.0-9E SW:v1.1.0.20
sysUpTime	6 Hours 42 Minutes 5 Seconds
sysName	
sysLocation	
sysContact	

Copyright© 2000 Nortel Networks, Inc. All rights reserved.

Additional Java security

When you choose Summary > Switch View from the Main Menu, a Java Security window opens (Figure 26).

Figure 26 Java Security window



JavaScript or a Java applet from '**Rapid Logic, Inc.**' is requesting additional privileges.

Granting the following is **high risk**:

Contacting and connecting with other computers over a network

☐ Remember this decision

Identity verified by VeriSign, Inc.

➔ Click Grant to open the Switch View page.

To avoid having the Java Security open again within a session, click the Remember this decision box. However, when you reset the switch, the Java Security window opens.

MAC address-based security

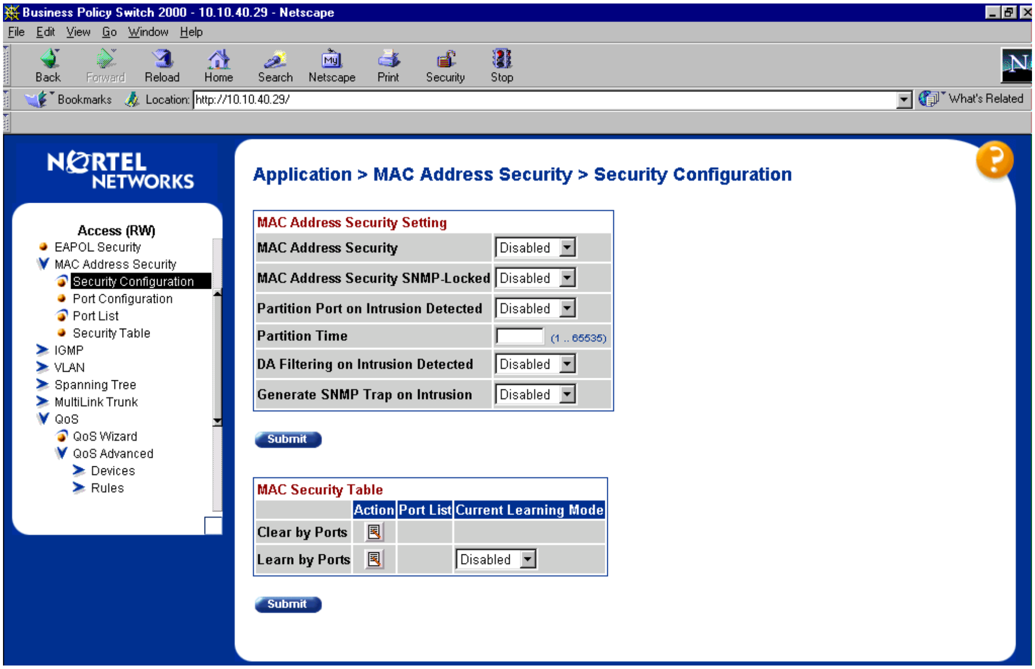
BPS 2000 software version 1.1 allows you to configure the MAC address-based security system using the Web-based management system. Using earlier software versions, you can configure this security with the CI menus. (For more information on MAC address-based security and configuring this feature, refer to *Using the Business Policy Switch 2000*.)

To configure MAC address-based security using the Web-based management system:

1. From the main menu of the Business Policy Switch 2000 Web-based management system, choose Application > MAC Address Security > Security Configuration.

   The MAC Address Security Configuration page opens (Figure 27).

Figure 27 MAC Address Security Configuration page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/ What's Related
NORTEL NETWORKS
Access (RW)
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Spanning Tree
MultiLink Trunk
QoS
QoS Wizard
QoS Advanced
Devices
Rules
Submit
Submit

Application > MAC Address Security > Security Configuration

MAC Address Security Setting

MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	(1 .. 65535)
DA Filtering on Intrusion Detected	Disabled
Generate SNMP Trap on Intrusion	Disabled

MAC Security Table

	Action	Port List	Current Learning Mode
Clear by Ports			
Learn by Ports			Disabled

2. In the MAC Address Security Setting area, choose Enabled in the MAC Address Security list and click Submit.

   If you want to lock the MAC Address Security SNMP feature, choose Enabled from the list.

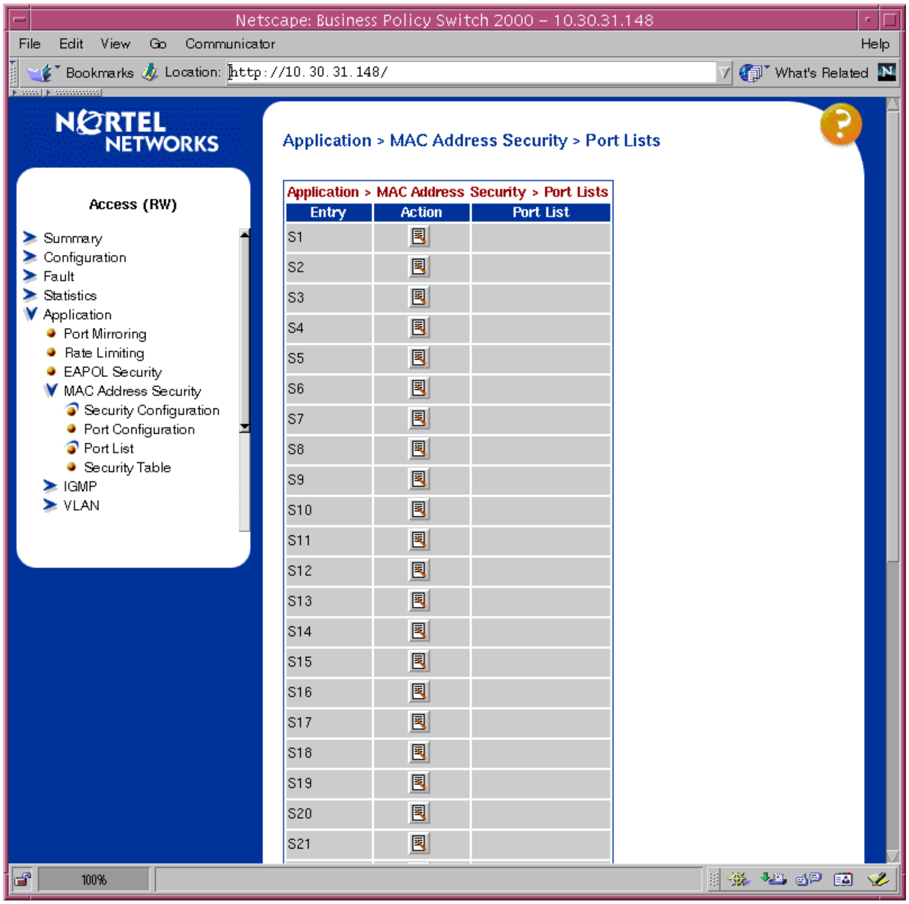
   If you want to partition a port when an intrusion is detected, choose Enabled (from Forever, Enabled, and Disabled choices) in the Partition Port on Intrusion Detected list, and type in the partition time in the Partition Time box. Only use the Partition Time box if Partition Port on Intrusion Detected is Enabled. (If you choose Forever from the list, that partition port is disabled until reset.)

If you want to isolate the intruding node, choose Enabled in the DA Filtering on Intrusion Detected list, and click Submit.

If you want an SNMP trap on intrusion, choose Enabled in the Generate SNMP Trap on Intrusion list.

3 Go to the MAC Address Security Port Lists page (Figure 28), and use the Action tab to configure each desired entry.

Figure 28 MAC Address Security Port Lists page

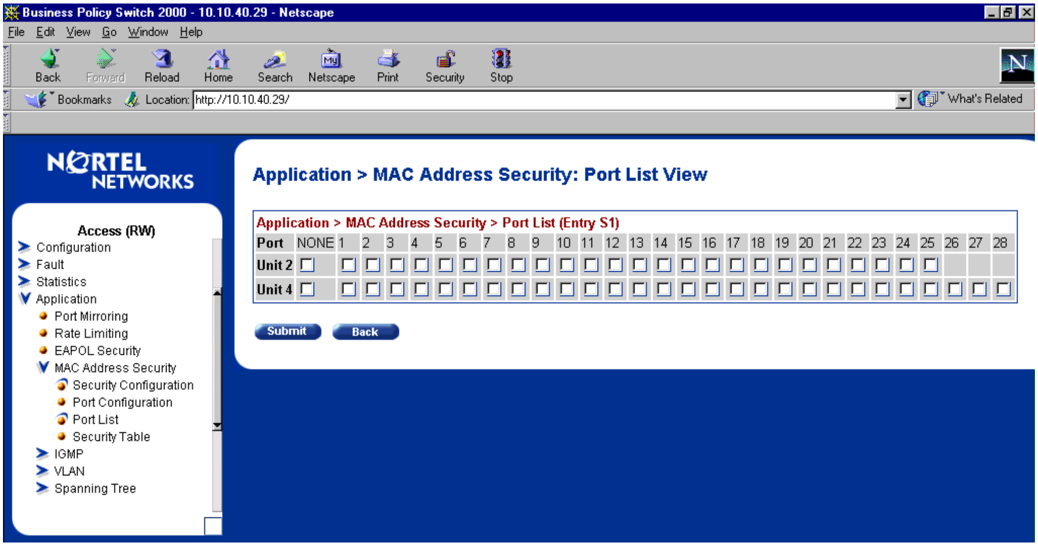

Netscape: Business Policy Switch 2000 – 10.30.31.148
File
Edit
View
Go
Communicator
Help
Bookmarks
Location: http://10.30.31.148/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Application > MAC Address Security > Port Lists
100%

Application > MAC Address Security > Port Lists

Entry	Action	Port List
S1	✎	
S2	✎	
S3	✎	
S4	✎	
S5	✎	
S6	✎	
S7	✎	
S8	✎	
S9	✎	
S10	✎	
S11	✎	
S12	✎	
S13	✎	
S14	✎	
S15	✎	
S16	✎	
S17	✎	
S18	✎	
S19	✎	
S20	✎	
S21	✎	

4 When you click the Action icon, the Ports List View, Port List page opens (Figure 29).

Figure 29 MAC Address Security Port List View, Port List page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Spanning Tree
Submit
Back

Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐			
Unit 4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

c Set the selected port for security enabled by clicking on the box under the port.

To disable security, click on the check mark that appears in the box, which will disappear.

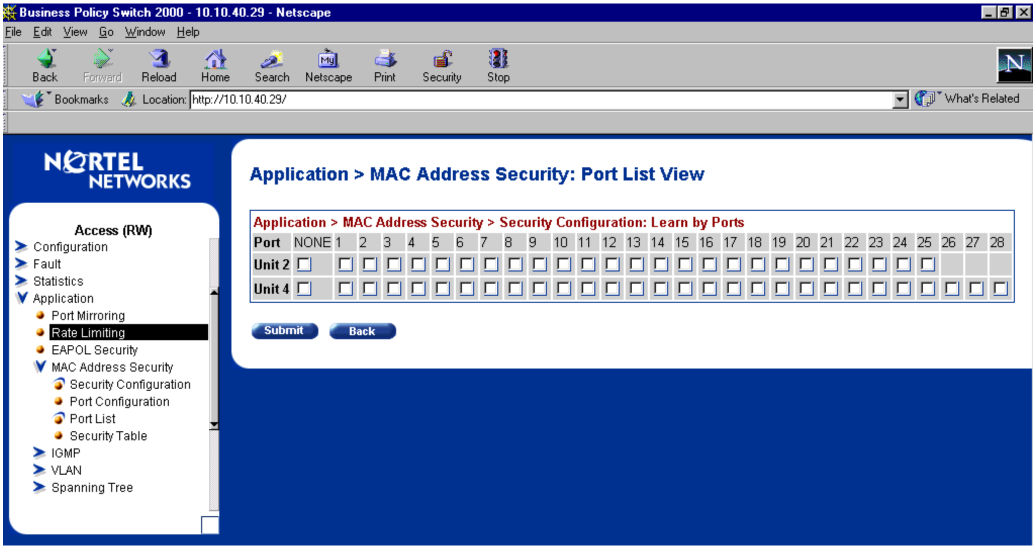
To have the entry available, but without any ports; click the box under None.

d Click Submit.

5 Return to the Security Configuration page (Figure 27), and click the Action icon in the Learn by Ports section.

The Ports List View, Learn by Ports page (Figure 30) opens.

Figure 30 MAC Address Security Port List View, Learn by Ports page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Spanning Tree
Submit
Back

Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Learn by Ports

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐			
Unit 4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

a Use this page to add or remove a specified port to the list of ports through which MAC addressed are learned.

To add a port, click on the box under the port number.

To delete a port, click on the check mark in the box under the port.

If you do not wish to add any ports, click in the box under None.

b Click Submit.

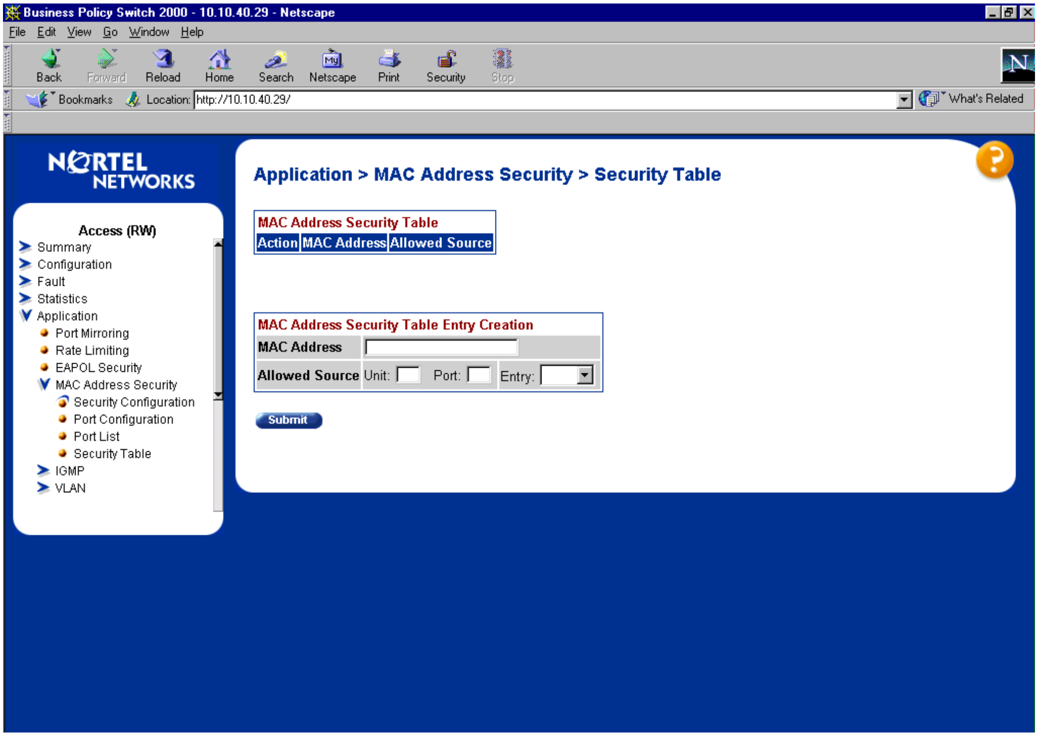
The Security Configuration page (Figure 27) opens.

6 Choose Enabled in the Learn by Ports list in the MAC Security Table section, at the bottom of the page

7 Click Security Table from Main Menu on the left under MAC Address Security.

The Security Table page opens (Figure 31).

Figure 31 MAC Address Security Table page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Submit

Application > MAC Address Security > Security Table

MAC Address Security Table

Action	MAC Address	Allowed Source

MAC Address Security Table Entry Creation

MAC Address	
Allowed Source	Unit: Port: Entry:

a Wait until the required addresses are learned.

b The MAC Address Security Table displays the addresses and the allowed source for each address.

8 To add a MAC address, in the MAC Address Security Table Entry Creation area:

a Enter the MAC address to which you want to allow access.

b To specify the entry though which the MAC address is allowed, either enter the unit/port number or choose the entry from the list.

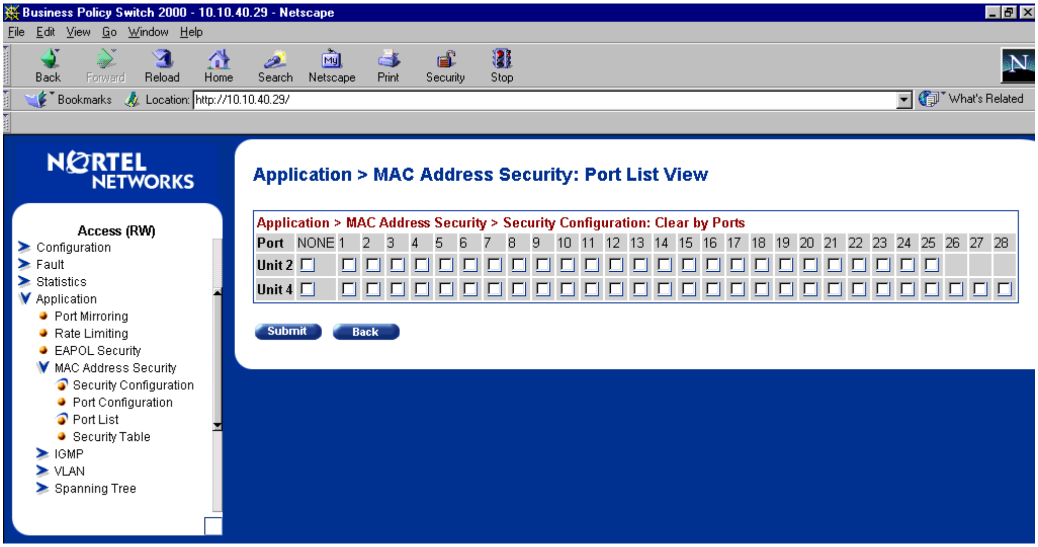
When you choose from the Entry list, you must have already selected ports for that entry by using the Port List View (Figure 32). However, if you choose the entry and do not want any ports on that entry, select None on the Port List View for that entry. If you select an entry in the MAC Address Security Table Entry Creation box and have not selected either any ports or the None option, the screen displays an error message saying that the Submit Failed.

c Click Submit.

9 To clear the information collected so far on the selected ports, return to the Security Configuration page (Figure 27), and click the Action icon in the Clear by Ports line in the MAC Security Table section, at the bottom of the Security Configuration page.

The Ports List View, Clear by Ports page (Figure 32) opens.

Figure 32 MAC Address Port List View, Clear By Ports page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Stop
Bookmarks
Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN
Spanning Tree
Submit
Back

Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Clear by Ports

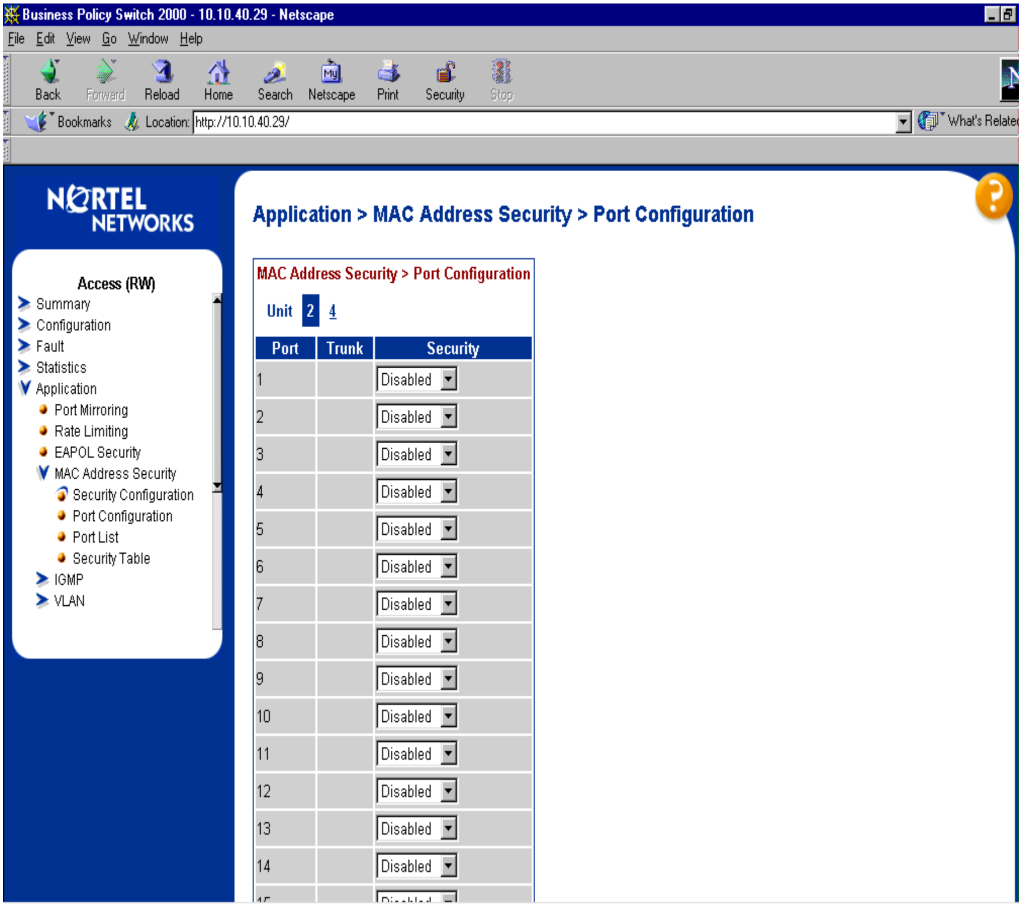
Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐			
Unit 4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

a Deselect the ports, and click Submit.

The Security Configuration page (Figure 27) opens.

10 Click Port Configuration from Main Menu on the left under MAC Address Security. The Port Configuration page opens (Figure 33).

Figure 33 MAC Address Security Port Configuration page


Business Policy Switch 2000 - 10.10.40.29 - Netscape
File Edit View Go Window Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://10.10.40.29/
What's Related
NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
Security Configuration
Port Configuration
Port List
Security Table
IGMP
VLAN

Application > MAC Address Security > Port Configuration

MAC Address Security > Port Configuration

Unit 2 4

Port	Trunk	Security
1		Disabled
2		Disabled
3		Disabled
4		Disabled
5		Disabled
6		Disabled
7		Disabled
8		Disabled
9		Disabled
10		Disabled
11		Disabled
12		Disabled
13		Disabled
14		Disabled

11 Set the security values for all desired ports to Enabled and click Submit.

The Port Configuration page also displays the Trunk Group membership for each port, if applicable.

Resolved issues

The following issues were resolved in version 1.1:

- You can download BayStack* 410 and BayStack 450 software images (and diagnostics) using the Device Manager in a mixed stack environment with Business Policy Switches.

  Using DM with a mixed stack and you choose Edit > File System, you can specify either the image for the BPS 2000 or the image for the BayStack, or both to download the software image(s).
- The BootP timeout for the BPS is now set to five minutes, which matches the BootP timeout value for the BayStack 450 switch. (CR 13161-1)
- BootP values set to either Always or When Needed are retained during a switch reset. (CR 126842-1)

The following issue was resolved in version 1.0.1:

- The ports on the BPS2000-4 TX MDA now autonegotiate correctly to 100 Mb/s full-duplex when they are connected to another BPS2000 port configured to autonegotiate.

Known issues

The following paragraphs discuss the known issues with the BPS 2000.

Version 1.1 issues

The following issues are known to be included in version 1.1 of the BPS 2000 software:

- The pre-defined Usernames for the login page of the Web-based management system are **uppercase** letters: RO or RW. (The documentation erroneously shows these user names as lower-case letters.) (CR 145225-1)
- The Multicast Group Membership table may display duplicate entries when the switch is in Distributed MultiLink Trunking (D-MLT) mode. However, the trunks function properly; this is a display problem only. (CR 138095-1)

- In a BPS 2000-only stack, the entire stack is reset to default values when you return the base unit to default values. (CR 145501-1)
- To disable a port that is part of a MultiLink Truck (MLT) group, use either Java Device Manager (JDM) or the Console Interface (CI) management system menus (you can use the Telnet connection). With the Web-based management system, you may be unable to disable ports that are part of MLTs. (CR 146607-1)
- When the High Speed Flow Control Autonegotiation feature is set to enabled (the default), the port only advertises support for 1000 Mb/s operation, in full-duplex mode. If you experience problems between the Business Policy Switch and other network devices, set Autonegotiation to *disabled* on both sides of the link.
- Gigabit MDA
  - When viewing Active Phy information from the console interface, the console must be connected to the unit containing the Gigabit MDA (the BayStack 450-1SR MDA and the BayStack 450-1LLR MDA) to display the appropriate Phy information. Incorrect information may be displayed if you connect to a unit not containing a Gigabit MDA.
  - When you remove a Gigabit MDA from a switch, the Active Phy of the effected unit displays the new status. However, occasionally, the Active Phys of the other units in the stack or remote units will not display the new status.

Known limitations

The following limitations are known to exist

- The current usable filters with software version 1.1 for the BPS are:
  - 50 policies
  - 200 IP filters and filter groups
  - 24 IP filters with same Source Address (18 nested subnets)
  - 14 Layer 2 filters and filter groups
  - 50 meters
  - 50 actions
  - Metered data consumes 2 filters

- Mixed stacks (hybrid stacks)—In order to upgrade BayStack 410 and BayStack 450 software in a hybrid stack, the stack must be fully redundant. All cables in the stack must be installed and operating properly. If the cables are not installed properly, the BayStack units will fail to upgrade. A message is displayed on consoles connected to BayStack 410 and BayStack 450 switches: `Primload Error - 2009 Switch will reset in 5 seconds...`
- You can configure as many as 63 protocol-based VLANs, with a sum total of "N" PID values not to exceed 15 (Table 11).

Table 11 Protocol and PID values

Protocol Name	Number of PID values (N)
Ip Ether2	2
Ipx 802.3	1
Ipx 802.2	1
Ipx Snap	2
Ipx Ether2Snap	2
AplTk Ether2Snap	2
Declat Ether2	1
DecOther Ether 2	10
Sna 802.2	2
Sna Ether2	1
NetBios 802.2	2
Xns Ether2	2
Vines Ether2	1
Ipv6 Ether2	1
Usrdef	1
Rarp Ether2	1

For more information on Predefined Protocol Identifiers (PIDs), hexadecimal values, and associated protocols, refer to *Using the Business Policy Switch 2000*.